Cycle lengths in finite groups and the size of the solvable radical

Alexander Bors[*]

June 15, 2015

Abstract

We prove the following: For any $\rho \in (0,1)$, if a finite group G has an automorphism with a cycle of length at least $\rho \cdot |G|$, then the index of the solvable radical $\mathrm{Rad}(G)$ in G is bounded from above in terms of ρ, and such a condition is strong enough to imply solvability of G if and only if $\rho > \frac{1}{10}$. Furthermore, considering, for exponents $e \in (0,1)$, the condition that a finite group G have an automorphism with a cycle of length at least $|G|^e$, such a condition is strong enough to imply $|\mathrm{Rad}(G)| \to \infty$ for $|G| \to \infty$ if and only if $e > \frac{1}{3}$. We also prove similar results for a larger class of bijective self-transformations of finite groups, so-called periodic affine maps.

1 Introduction

1.1 Motivation and main results

In the author's preprint [1], we studied how having an automorphism with a "long" cycle restricts the structure of finite groups. One of the main results was that a finite group G with an automorphism one of whose cycles has length greater than $\frac{1}{2}|G|$ is necessarily abelian. For proving these (and other) results, it turned out to be fruitful to study not only largest possible cycle lengths of automorphisms of finite groups G, but also of a more general type of bijective self-transformations, namely maps $\mathrm{A}_{g_0,\alpha}: G \to G$ of the form $g \mapsto g_0\alpha(g)$ for some fixed $g_0 \in G$ and automorphism α of G. We called these maps *periodic (left-)affine maps of* G.

Although most of the techniques introduced in [1] work under weaker assumptions as well, one important idea (that an automorphism cycle, in a finite group G with $|G| \geq 3$, of length at least $\frac{1}{2}|G|$ must intersect with its pointwise inverse) makes explicit use of the fraction $\frac{1}{2}$, and it is not clear how one could derive similar results under the assumption that G have an automorphism cycle of length at least, say, $\frac{1}{3}|G|$.

We will tackle this problem here by studying consequences of conditions on finite groups G of the form "G has an automorphism cycle of length at least $\rho|G|$" ("first kind") and "G has a periodic affine map cycle of length at least $\rho|G|$" ("second kind") for some fixed $\rho \in (0,1)$, and also of the form "G has an automorphism cycle of length at least $|G|^e$" ("third kind") and "G has a periodic affine map cycle of length at least $|G|^e$" ("fourth kind") for some fixed $e \in (0,1)$. Our main results, all of which rely on the classification of finite simple groups (CFSG), are as follows:

Theorem 1.1.1. *Let $\rho \in (0,1)$ be fixed, let G be a finite group, and denote by* $\mathrm{Rad}(G)$ *the solvable radical of G. Then:*
(1) If G has an automorphism cycle of length at least $\rho|G|$, then $[G : \mathrm{Rad}(G)] \leq \rho^{E_1}$, where $E_1 = -1.778151\ldots$.

[*] University of Salzburg, Mathematics Department, Hellbrunner Straße 34, 5020 Salzburg, Austria.
E-mail: alexander.bors@sbg.ac.at

The author is supported by the Austrian Science Fund (FWF): Project F5504-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

2010 *Mathematics Subject Classification*: primary: 20B25, 20D25, 20D45, secondary: 20D05, 20E22, 20G40, 37P99.

Key words and phrases: finite groups, cycle structure, solvable radical, semisimple groups

(2) If G has a periodic affine map cycle of length at least $\rho|G|$, then $[G:\mathrm{Rad}(G)]\leq\rho^{E_2}$, where $E_2=-5.906890\ldots$.

So finite groups satisfying a condition of one of the first two forms are "not too far from being solvable". An interesting question is for which values of ρ such a condition actually implies solvability. Note that by [1, Theorem 1.1.7], for conditions of the first form, this is the case whenever $\rho>\frac{1}{2}$. However, since solvability is a weaker condition than abelianity, one may hope to be able to do better, and actually, we will prove:

Corollary 1.1.2. *Let G be a finite group.*
(1) If G has an automorphism cycle of length greater than $\frac{1}{10}|G|$, then G is solvable. On the other hand, the alternating group $\mathcal{A}_5$ has an automorphism cycle of length $6=\frac{1}{10}|\mathrm{A}_5|$.
(2) If G has a periodic affine map cycle of length greater than $\frac{1}{4}|G|$, then G is solvable. On the other hand, $\mathcal{A}_5$ has a periodic affine map cycle of length $15=\frac{1}{4}|\mathcal{A}_5|$.

As for the conditions of the third and fourth kind mentioned above, we cannot expect results as strong as Theorem 1.1.1 (see the discussion after Lemma 2.1.1), but we have the following:

Theorem 1.1.3. *(1) Let $\epsilon>0$ be fixed. Then for every $\xi>0$, there exists a constant $K(\epsilon,\xi)$ such that for all finite groups G having an automorphism cycle of length at least $|G|^{\frac{1}{3}+\epsilon}$, we have $[G:\mathrm{Rad}(G)]\leq\max(K(\epsilon,\xi),|G|^{1-\frac{3}{2}\epsilon+\xi})$. In particular, under a condition of the third kind with $e:=\frac{1}{3}+\epsilon$, for all $\xi>0$, we have $|G|^{\frac{3}{2}\epsilon-\xi}=o(|\mathrm{Rad}(G)|)$ for $|G|\to\infty$.*
(2) Let $\epsilon>0$ be fixed. Then for every $\xi>0$, there exists a constant $K_{\mathrm{aff}}(\epsilon,\xi)$ such that for all finite groups G having a periodic affine map cycle of length at least $|G|^{\frac{2}{3}+\epsilon}$, we have $[G:\mathrm{Rad}(G)]\leq\max(K_{\mathrm{aff}}(\epsilon,\xi),|G|^{1-3\epsilon+\xi})$. In particular, under a condition of the fourth kind with $e:=\frac{2}{3}+\epsilon$, for all $\xi>0$, we have $|G|^{3\epsilon-\xi}=o(|\mathrm{Rad}(G)|)$ for $|G|\to\infty$.
(3) There exists a sequence $(G_n)_{n\in\mathbb{N}}$ of finite groups G_n such that $|\mathrm{Rad}(G_n)|=1$ for all $n\in\mathbb{N}$, $|G_n|\to\infty$ for $n\to\infty$, and for all $n\in\mathbb{N}$, G_n has an automorphism cycle of length greater than $|G_n|^{\frac{1}{3}}$ and a periodic affine map cycle of length greater than $|G_n|^{\frac{2}{3}}$.

We remark that we can and will give explicit definitions for $K(\epsilon,\xi)$, $K_{\mathrm{aff}}(\epsilon,\xi)$ and the sequence $(G_n)_{n\in\mathbb{N}}$, see the proof of Theorem 1.1.3 at the end of Section 3.

1.2 Outline

In Section 2, we present the technical tools needed for proving our main results, some of which were already introduced in [1] and are therefore given without proof here. None of them make use of the CFSG. It turns out that using (part of) these tools, the proof of all of the main results can be reduced to the proof of one technical lemma, namely Lemma 3.1, which we will call the "main lemma". It is a statement about maximum cycle lengths of automorphisms and of periodic affine maps of finite nonabelian characteristically simple groups, and its proof will use the CFSG. Section 3 shows how the main lemma implies all the main results, and Section 4 consists of the proof of the main lemma.

1.3 Notation and terminology

For the readers' convenience, we explain those parts of our notation that may be nonstandard. We denote by $\mathbb{N}$ the set of natural numbers (von Neumann ordinals, including 0), and by $\mathbb{N}^+$ the set of positive integers. The image of a set M under a function f is denoted by $f[M]$. The identity function on a set M is denoted by id_M, and the symmetric group on M is denoted by $\mathcal{S}_M$, except when M is a natural number n, in which case we set $\mathcal{S}_n:=\mathcal{S}_{\{1,\ldots,n\}}$. Similarly, for a natural number n, $\mathcal{A}_n$ is the alternating group on $\{1,\ldots,n\}$.

Let G be a group. For an element $r\in G$, we denote by $\tau_r:G\to G,g\mapsto rgr^{-1}$ the inner automorphism of G with respect to r. The centralizer and normalizer of a subset $X\subseteq G$ are denoted by $\mathrm{C}_G(X)$ and $\mathrm{N}_G(X)$ respectively. As in Theorems 1.1.1 and 1.1.3, $\mathrm{Rad}(G)$ denotes the solvable radical of G. For linguistical simplicity, we will frequently use the following notation, see also [1, Definitions 1.1.1, 2.1.1 and 2.1.2] as well as [5]:

Definition 1.3.1. *(1) Let ψ be a permutation of a finite set X. We denote by $\Lambda(\psi)$ the maximum length of one of the disjoint cycles into which ψ decomposes, and set $\lambda(\psi) := \frac{1}{|X|}\Lambda(\psi)$.*
(2) For a finite group G, we set $\Lambda(G) := \max_{\alpha\in\mathrm{Aut}(G)}\Lambda(\alpha)$ and $\lambda(G) := \frac{1}{|G|}\Lambda(G)$.
(3) For a finite group G, the group of periodic left-affine maps of G is denoted by $\mathrm{Aff}(G)$. We set $\Lambda_{\mathrm{aff}}(G) := \max_{A\in\mathrm{Aff}(G)}\Lambda(A)$ and $\lambda_{\mathrm{aff}}(G) := \frac{1}{|G|}\Lambda_{\mathrm{aff}}(G)$.
(4) For a finite group G, we denote by $\mathrm{meo}(G)$ the maximum element order of G and set $\mathrm{mao}(G) := \mathrm{meo}(\mathrm{Aut}(G))$, the maximum automorphism order of G.

We also use some notation and terminology from the theory of finite dynamical systems:

Definition 1.3.2. *(1) A **finite dynamical system**, abbreviated henceforth by **FDS**, is a finite set X together with a map $f: X\to X$ (a so-called **self-transformation of** X). It is called **periodic** if and only if f is bijective.*
*(2) If $(X_1,f_1),\ldots,(X_r,f_r)$ are FDSs, their **product** is defined as the FDS $(X_1\times\cdots\times X_r, f_1\times\cdots\times f_r)$, where $f_1\times\cdots\times f_r$ is the self-transformation of $X_1\times\cdots\times X_r$ mapping $(x_1,\ldots,x_r)\mapsto(f_1(x_1),\ldots,f_r(x_r))$.*
(3) If (X,ψ) is a periodic FDS and $x\in X$, we denote the length of the cycle of x under ψ by $\mathrm{cl}_{\psi}(x)$.

Finally, in this paper, exp mostly denotes the exponent of a group, although in the definition of Ψ in Subsection 2.4, it denotes the natural exponential function. log always denotes the natural logarithm, and for $c>1$, the logarithm with base c is denoted by $\log_c$.

2 Some tools

2.1 Lemmata concerning maximum cycle lengths

Lemma 2.1.1 below was used in the proof of [1, Lemma 2.1.6], of which Lemma 2.1.2 is a part.

Lemma 2.1.1. *Let $(X_1,\psi_1),\ldots,(X_r,\psi_r)$ be periodic FDSs, and let $x=(x_1,\ldots,x_r)\in X_1\times\cdots\times X_r$. Then $\mathrm{cl}_{\psi_1\times\cdots\times\psi_r}(x)=\mathrm{lcm}(\mathrm{cl}_{\psi_1}(x_1),\ldots,\mathrm{cl}_{\psi_r}(x_r))$. In particular, $\Lambda(\psi_1\times\cdots\times\psi_r)\leq\Lambda(\psi_1)\cdots\Lambda(\psi_r)$.* □

We remark that by Lemma 2.1.1, any condition on finite groups G of the form $\lambda(G)\geq f(|G|)$, where $f:\mathbb{N}^+\to[0,1]$ is such that $f(n)\to 0$ for $n\to\infty$, is not strong enough to imply that the index $[G:\mathrm{Rad}(G)]$ is bounded from above. Indeed, under such a condition, any finite group G_0 (in particular, any nonabelian finite simple group G_0) may occur as a direct factor of G. To see this, let p be a prime which is so large that $f(p|G_0|)\leq\frac{1}{2|G_0|}$. Considering the product automorphism $\mathrm{id}_{G_0}\times\alpha$ of $G:=G_0\times\mathbb{Z}/p\mathbb{Z}$, where $\alpha\in\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ is the multiplication by any primitive root modulo p, it is not difficult to see by Lemma 2.1.1 that

$$\lambda(G)\geq\lambda(\mathrm{id}_{G_0}\times\alpha)=\frac{p-1}{p|G_0|}=(1-\frac{1}{p})\cdot\frac{1}{|G_0|}\geq\frac{1}{2|G_0|}\geq f(|G|).$$

As in [1], we say that a family $(G_i)_{i\in I}$ of groups has the *splitting property* if and only if for every automorphism α of $\prod_{i\in I}G_i$, there exists a family $(\alpha_i)_{i\in I}$ such that α_i is an automorphism of G_i for $i\in I$, and $\alpha((g_i)_{i\in I})=(\alpha_i(g_i))_{i\in I}$ for all $(g_i)_{i\in I}\in\prod_{i\in I}G_i$.

Lemma 2.1.2. *Let $(G_1,\ldots,G_r)$ be a tuple of finite groups with the splitting property. Then:*
(1) $\Lambda(G_1\times\cdots\times G_r)\leq\Lambda(G_1)\cdots\Lambda(G_r)$.
(2) For every periodic affine map A of $G_1\times\cdots\times G_r$, there exists a tuple $(A_1,\ldots,A_r)$ such that $A_i\in\mathrm{Aff}(G_i)$ for $i=1,\ldots,r$ and $A=A_1\times\cdots\times A_r$. In particular, $\Lambda_{\mathrm{aff}}(G_1\times\cdots\times G_r)\leq\Lambda_{\mathrm{aff}}(G_1)\cdots\Lambda_{\mathrm{aff}}(G_r)$. □

The following is a part of [1, Lemma 2.1.4]:

Lemma 2.1.3. *Let G be a finite group, N a characteristic subgroup of G. Then:*
(1) $\Lambda(G)\leq\Lambda_{\mathrm{aff}}(N)\cdot\Lambda(G/N)$, or equivalently, $\lambda(G)\leq\lambda_{\mathrm{aff}}(N)\cdot\lambda(G/N)$. In particular, $\lambda(G/N)\geq\lambda(G)$.
(2) $\Lambda_{\mathrm{aff}}(G)\leq\Lambda_{\mathrm{aff}}(N)\cdot\Lambda_{\mathrm{aff}}(G/N)$, or equivalently, $\lambda_{\mathrm{aff}}(G)\leq\lambda_{\mathrm{aff}}(N)\cdot\lambda_{\mathrm{aff}}(G/N)$. In particular, $\lambda_{\mathrm{aff}}(G)\leq\min(\lambda_{\mathrm{aff}}(N),\lambda_{\mathrm{aff}}(G/N))$. □

We will now prove some more results that are useful for the study of Λ_{aff}-values of finite groups. For a more concise formulation, we define:

Definition 2.1.4. *Let G be a finite group, $x \in G$, α an automorphism of G, $n \in \mathbb{N}^+$.*
*(1) The element $\mathrm{sh}_\alpha^{(n)}(x) := x\alpha(x)\cdots\alpha^{n-1}(x) \in G$ is called the **n-th shift of x under** α.*
*(2) The element $\mathrm{sh}_\alpha(x) := \mathrm{sh}_\alpha^{(\mathrm{ord}(\alpha))} \in G$ is called the **shift of x under** α.*

The following calculation rules for shifts are easy to show:

Lemma 2.1.5. *Let G be a finite group, $x \in G$, α an automorphism of G.*
(1) $\alpha(\mathrm{sh}_\alpha(x)) = x\,\mathrm{sh}_\alpha(x)x^{-1}$.
(2) If $d \in \mathbb{N}^+$ is such that $\mathrm{cl}_\alpha(x) \mid d \mid \mathrm{ord}(\alpha)$, then $\mathrm{sh}_\alpha(x) = \mathrm{sh}_\alpha^{(d)}(x)^{\frac{\mathrm{ord}\,\alpha}{d}}$. □

Definition 2.1.4 is motivated by the following: It is well-known that there is natural isomorphism between $\mathrm{Aff}(G)$, the product, inside $\mathcal{S}_G$, of the image of the left regular representation of G with $\mathrm{Aut}(G)$, and the holomorph of G, $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$. The isomorphism is simply given by the map $\mathrm{Aff}(G) \to \mathrm{Hol}(G), \mathrm{A}_{x,\alpha} \mapsto (x,\alpha)$. It is therefore clear that $\mathrm{ord}(\alpha) \mid \mathrm{ord}(\mathrm{A}_{x,\alpha})$ for all $x \in G$ and all $\alpha \in \mathrm{Aut}(G)$, and thus $\mathrm{ord}(\mathrm{A}_{x,\alpha}) = \mathrm{ord}(\alpha) \cdot \mathrm{ord}(\mathrm{A}_{x,\alpha}^{\mathrm{ord}(\alpha)})$. However, easy computations reveal that under said natural isomorphism, $\mathrm{A}_{x,\alpha}^{\mathrm{ord}(\alpha)}$ corresponds to the element $\mathrm{sh}_\alpha(x) \in G$. This shows that in general, we have the following formula for computing orders of periodic affine maps of finite groups:

$$\mathrm{ord}(\mathrm{A}_{x,\alpha}) = \mathrm{ord}(\alpha) \cdot \mathrm{ord}(\mathrm{sh}_\alpha(x)).$$

When ψ is a permutation of a finite set X and $n \in \mathbb{N}^+$, we say that an orbit O of the action of ψ on X *induces* an orbit $\tilde{O}$ of ψ^n (or that $\tilde{O}$ *stems from* O) if and only if $\tilde{O} \subseteq O$, in which case $|\tilde{O}| = \frac{1}{\gcd(n,|O|)}|O|$. Every orbit of ψ induces an orbit of ψ^n, and every orbit of ψ^n stems from precisely one orbit of ψ.

Lemma 2.1.6. *Let G be a finite group, $x \in G$, α an automorphism of G. Then every cycle length of $\mathrm{A}_{x,\alpha}$ is divisible by $\mathrm{L}_G(x,\alpha) := \mathrm{ord}(\mathrm{sh}_\alpha(x)) \cdot \prod_p p^{\nu_p(\mathrm{ord}(\alpha))}$, where p runs through the common prime divisors of $\mathrm{ord}(\mathrm{sh}_\alpha(x))$ and $\mathrm{ord}(\alpha)$. In particular, $\mathrm{L}_G(x,\alpha) \mid |G|$.*

Proof. Every orbit of $\mathrm{A}_{x,\alpha}^{\mathrm{ord}(\alpha)}$, the left multiplication by $\mathrm{sh}_\alpha(x)$ in G, has size $\mathrm{ord}(\mathrm{sh}_\alpha(x))$, so certainly every cycle length of $\mathrm{A}_{x,\alpha}$ is divisible by $\mathrm{ord}(\mathrm{sh}_\alpha(x))$. In particular, if p is a common prime divisor of $\mathrm{ord}(\mathrm{sh}_\alpha(x))$ and $\mathrm{ord}(\alpha)$, and O is any orbit of $\mathrm{A}_{x,\alpha}$, then $p \mid |O|$, but $p^{\nu_p(\mathrm{ord}(\mathrm{sh}_\alpha(x)))}$ still divides $|\tilde{O}|$, where $\tilde{O}$ is the orbit of $\mathrm{A}_{x,\alpha}^{\mathrm{ord}(\alpha)}$ induced by O. This is only possible if $|O|$ actually is divisible by $p^{\nu_p(\mathrm{ord}(\mathrm{sh}_\alpha(x)))+\nu_p(\mathrm{ord}(\alpha))}$, and the assertion follows. □

Lemma 2.1.7. *Let G be a finite group, $x, r \in G$. Then $x^{-1}r \in \mathrm{C}_G(\mathrm{sh}_{\tau_r}(x))$. In particular, if, for some subgroup $H \leq G$, $\mathrm{C}_G(\mathrm{sh}_{\tau_r}(x)) \subseteq H$, then $x \in H$ if and only if $r \in H$.*

Proof. This follows immediately from $r\,\mathrm{sh}_{\tau_r}(x)r^{-1} = \tau_r(\mathrm{sh}_{\tau_r}(x)) = x\,\mathrm{sh}_{\tau_r}(x)x^{-1}$, where the first equality is by the definition of τ_r and the second by Lemma 2.1.5(1). □

Lemma 2.1.8. *(1) Let G be a finite centerless group, $r, s \in G$. Set $x := sr^{-1}$. Then $\mathrm{sh}_{\tau_r}(x) = s^{\mathrm{ord}(r)}$. In particular, $\mathrm{ord}(\mathrm{A}_{x,\tau_r}) = \mathrm{lcm}(\mathrm{ord}(s), \mathrm{ord}(r))$.*
(2) Let G be any finite group, $r, s \in G$, x as in point (1). Then $\mathrm{sh}_{\tau_r}(x) = s^{\mathrm{ord}(\tau_r)} \cdot r^{-\mathrm{ord}(\tau_r)}$. In particular, if $\gcd(\mathrm{ord}(r), \mathrm{ord}(s)) = 1$, then $\mathrm{ord}(\mathrm{A}_{x,\tau_r}) = \mathrm{ord}(s) \cdot \mathrm{ord}(r)$.

Proof. An easy induction on $n \in \mathbb{N}^+$ proves that in both cases, we have $\mathrm{sh}_{\tau_r}^{(n)}(x) = s^n r^{-n}$. Therefore, we have $\mathrm{sh}_{\tau_r}(x) = s^{\mathrm{ord}(r)}$ under the assumptions of point (1). This implies that

$$\mathrm{ord}(\mathrm{A}_{x,\tau_r}) = \mathrm{ord}(\tau_r) \cdot \mathrm{ord}(\mathrm{sh}_{\tau_r}(x)) = \mathrm{ord}(r) \cdot \frac{\mathrm{ord}(s)}{\gcd(\mathrm{ord}(s), \mathrm{ord}(r))} = \mathrm{lcm}(\mathrm{ord}(s), \mathrm{ord}(r)),$$

proving the statement of point (1). The proof of point (2) is similar, using that $r^{-\mathrm{ord}(\tau_r)} \in \zeta G$ and that the order of a product of two commuting elements with coprime orders is the product of their orders. □

2.2 Some results on finite semisimple groups

In this Subsection, for the readers' convenience, we first briefly recall some basic facts on finite semisimple groups (finite groups without nontrivial solvable normal subgroups) which we will need later, following mostly the exposition in [9, pp. 89ff.]. Afterward, we generalize a result of Horoševskiĭ on largest cycle lengths of automorphisms of finite semisimple groups to periodic affine maps of such groups.

Any group G has a unique largest normal centerless CR-subgroup, the centerless CR-radical of G, which we denote by $\mathrm{CRRad}(G)$. From now on, assume that G is finite and semisimple. Then $\mathrm{CRRad}(G)$ coincides with $\mathrm{Soc}(G)$, the socle of G. G canonically embeds into $\mathrm{Aut}(\mathrm{Soc}(G))$ by its conjugation action (which shows that for any finite centerless CR-group R, there are only finitely many isomorphism types of finite semisimple groups G such that $\mathrm{Soc}(G) \cong R$), and the image G^* of this embedding clearly contains $\mathrm{Inn}(\mathrm{Soc}(G))$. Conversely, for every finite centerless CR-group R, any group G such that $\mathrm{Inn}(R) \leq G \leq \mathrm{Aut}(R)$ is semisimple.

If $S_1, \ldots, S_r$ are pairwise nonisomorphic nonabelian finite simple groups, and $n_1, \ldots, n_r \in \mathbb{N}^+$, then the tuple $(S_1^{n_1}, \ldots, S_r^{n_r})$ has the splitting property. In particular, $\mathrm{Aut}(S_1^{n_1} \times \cdots \times S_r^{n_r}) = \mathrm{Aut}(S_1^{n_1}) \times \cdots \times \mathrm{Aut}(S_r^{n_r})$. The structure of the automorphism groups of finite nonabelian characteristically simple groups (powers of finite nonabelian simple groups) can be described by permutational wreath products. More precisely, $\mathrm{Aut}(S^n) = \mathrm{Aut}(S) \wr \mathcal{S}_n$ for any finite nonabelian simple group S and any $n \in \mathbb{N}^+$.

Rose [10, Lemma 1.1] observed that, in generalization of the embedding of G into $\mathrm{Aut}(\mathrm{Soc}(G))$ for finite semisimple groups G, if G is any group, and H a characteristic subgroup of G such that $\mathrm{C}_G(H) = \{1_G\}$, then G embeds into $\mathrm{Aut}(H)$ by its conjugation action on H, and, viewing G as a subgroup of $\mathrm{Aut}(H)$, $\mathrm{Aut}(G)$ is canonically isomorphic to $\mathrm{N}_{\mathrm{Aut}(H)}(G)$. This implies, among other things, that automorphism groups of finite centerless CR-groups are complete.

Let us now turn to the aforementioned theorem of Horoševskiĭ. Following the terminology from [4], we define:

Definition 2.2.1. *Let ψ be a permutation of a finite set. A cycle of ψ whose length equals $\mathrm{ord}(\psi)$ is called a **regular cycle of** ψ.*

Thus a permutation ψ of a finite set has a regular cycle if and only if $\Lambda(\psi) = \mathrm{ord}(\psi)$. In the case of periodic affine maps A of finite groups G, the order is often easier to compute than the Λ-value, since for computing the order, one can work with the compact representation $A = \mathrm{A}_{x,\alpha}$ for appropriate $x \in G$ and $\alpha \in \mathrm{Aut}(G)$, and composition of periodic affine maps translates, on the level of the compact representations, into some simple manipulations (by the isomorphism $\mathrm{Aff}(G) \to \mathrm{Hol}(G)$ mentioned above), without the need to "spread out" the entire element structure of G to determine the cycle lengths of the elements of G under A.

In view of this, it would be nice to know at least for some classes of finite groups G that all periodic affine maps of G have a regular cycle to make computation of Λ- and Λ_{aff}-values easier. Indeed, Horoševskiĭ proved:

Theorem 2.2.2. *([6, Theorem 1]) Let G be a finite semisimple group. Then every automorphism of G has a regular cycle.* □

We will extend this to:

Theorem 2.2.3. *Let G be a finite semisimple group. Then every periodic affine map of G has a regular cycle.*

Our proof of Theorem 2.2.3 is mostly an adaptation of Horoševskiĭ's proof of Theorem 2.2.2, with the arguments getting slightly more complicated because of the more general situation. However, at one point, our proof significantly differs from the one of Horoševskiĭ, using the recent result [4, Theorem 3.2] to settle one important case. Just like Horoševskiĭ, we use the following:

Lemma 2.2.4. *Let X be a finite set, $\psi \in \mathcal{S}_X$, p a prime such that $p^2 \mid \mathrm{ord}(\psi)$. The following are equivalent:*
(1) ψ has a regular cycle.
(2) ψ^p has a regular cycle.

Proof. See [6, Lemma 1]. The assumption there that ψ (called ϕ there) is an automorphism of a finite group is not needed. □

Before we continue with the next lemma, a quick reminder and an easy observation: Recall that for a group G, an automorphism α of G, and a normal subgroup $N \trianglelefteq G$, α-admissibility of N (i.e., the property that $\alpha(N) = N$) is equivalent to the existence of an automorphism $\tilde{\alpha}$ of G/N such that, denoting by $\pi : G \to G/N$ the canonical projection, $\pi \circ \alpha = \tilde{\alpha} \circ \pi$. In this case, $\tilde{\alpha}$ is unique and is called the *automorphism of G/N induced by α*. More generally, if, for some permutation ψ of G, there exists a permutation σ of G/N such that $\pi \circ \psi = \sigma \circ \pi$, we still call σ *induced by ψ*. It is not difficult to see that for any group G, any $N \trianglelefteq G$ and any periodic affine map $A = \mathrm{A}_{x,\alpha}$ of G, A induces a permutation $\tilde{A}$ of G/N if and only if N is α-admissible, and in this case, $\tilde{A}$ is a periodic affine map of G/N; actually, $\tilde{A} = \mathrm{A}_{\pi(x),\tilde{\alpha}}$.

Lemma 2.2.5. *Let G be a group, $B \trianglelefteq G$, A a periodic affine map of G such that $A_{|B} = \mathrm{id}_B$. Then $\mathrm{C}_G(B) \trianglelefteq G$, and A induces the identity map in $G/\mathrm{C}_G(B)$.*

Proof. In general, for all $x \in G$ and $\alpha \in \mathrm{Aut}(G)$, it follows immediately from the definition of $\mathrm{A}_{x,\alpha}$ that $\mathrm{A}_{x,\alpha}(1_G) = x$. Since $A(1_G) = 1_G$ by assumption, A thus actually is an automorphism of G, so the claim follows from [6, Lemma 2]. □

Lemma 2.2.6. *Let $X_1, \ldots, X_n$ be finite sets, ψ_i, $i = 1, \ldots, n$, a permutation of X_i with a regular cycle. Then $\psi_1 \times \cdots \times \psi_n$ has a regular cycle.* □

One additional easy observation which we will need is the following:

Lemma 2.2.7. *Let G be a group, $A = \mathrm{A}_{x,\alpha}$ a periodic left affine map of G such that $\mathrm{fix}(A) \neq \emptyset$. Then $\mathrm{fix}(A)$ is a left coset of the subgroup $\mathrm{fix}(\alpha) \leq G$.*

Proof. For all $g \in G$, we have that $g \in \mathrm{fix}(A)$ if and only if $x\alpha(g) = g$, or $x = g\alpha(g)^{-1}$. Therefore, if we fix $f \in \mathrm{fix}(A)$, then $\mathrm{fix}(A)$ can be desribed as $\{g \in G \mid g\alpha(g)^{-1} = f\alpha(f)^{-1}\} = \{g \in G \mid g^{-1}f \in \mathrm{fix}(\alpha)\} = f\,\mathrm{fix}(\alpha)$. □

Proof of Theorem 2.2.3. The proof is by induction on $|G|$, the induction base $|G| = 1$ being trivial, with an inner induction on $\mathrm{ord}(A)$, the induction base $\mathrm{ord}(A) = 1$ being trivial. For the induction step, assume that $A = \mathrm{A}_{x,\alpha}$ is a periodic affine map of the finite semisimple group G. To show that A has a regular cycle, we make a case distinction:

1. Case: G is simple. This case is by contradiction, so assume that A does not have a regular cycle. Note that by Lemma 2.2.4 and the induction hypothesis, $\mathrm{ord}(A)$ then must be squarefree, say $\mathrm{ord}(A) = p_1 \cdots p_r$, with the p_i pairwise distinct primes. Since by the induction hypothesis, A^{p_1} has a cycle of length $\mathrm{ord}(A^{p_1}) = p_2 \cdots p_r$, but A has no regular cycle, A must also have a cycle of length $p_2 \cdots p_r$, which implies $p_2 \cdots p_r < |G|$. Now note that by the assumption that A does not have a regular cycle, we have $G \subseteq \bigcup_{i=1}^{r} \mathrm{fix}(A^{\prod_{j \neq i} p_j})$. By Lemma 2.2.7, denoting by α_i the underlying automorphism of $A^{\prod_{j \neq i} p_j}$, we have $|\mathrm{fix}(A^{\prod_{j \neq i} p_j})| = |\mathrm{fix}(\alpha_i)|$, and so there must exist $i \in \{1, \ldots, r\}$ such that $[G : \mathrm{fix}(\alpha_i)] \leq r$ (otherwise, G could not be covered by the r fixed point sets above). But since G is simple, this implies that $|G| \leq r! \leq p_2 \cdots p_r < |G|$, a contradiction.

2. Case: G is characteristically simple, but not simple. Let S be a nonabelian finite simple group and $n \geq 2$ such that $G \cong S^n$. α is an element of the permutational wreath product $\mathrm{Aut}(S) \wr \mathcal{S}_n$, i.e., α is a composition $(\alpha_1 \times \cdots \times \alpha_n) \circ \psi$, where each α_i is an automorphism of S and ψ is a permutation of coordinates on S^n. Writing $x = (x_1, \ldots, x_n)$, and denoting by μ_x the left multiplication by x in S^n, it follows that $A = \mu_x \circ ((\alpha_1 \times \cdots \times \alpha_n) \circ \psi) = ((\mu_{x_1} \times \cdots \times \mu_{x_n}) \circ (\alpha_1 \times \cdots \times \alpha_n)) \circ \psi = (\mathrm{A}_{x_1,\alpha_1} \times \cdots \times \mathrm{A}_{x_n,\alpha_n}) \circ \psi$. This proves that $A \in \mathrm{Aff}(S) \wr \mathcal{S}_n$ (actually, we just proved that $\mathrm{Aff}(S^n) = \mathrm{Aff}(S) \wr \mathcal{S}_n$). By induction hypothesis, every permutation from $\mathrm{Aff}(S)$ has a regular cycle, and so by [4, Theorem 3.2], A has a regular cycle.

3. Case: G is completely reducible, but not characteristically simple. Let $S_1, \ldots, S_r$ be pairwise nonisomorphic nonabelian finite simple groups, $n_1, \ldots, n_r \in \mathbb{N}^+$ such that $G \cong S_1^{n_1} \times \cdots \times S_r^{n_r}$, and note that $r \geq 2$ by assumption. Since $(S_1^{n_1}, \ldots, S_r^{n_r})$ has the splitting property, by Lemma 2.1.2(2), A can be written as a product of periodic affine maps over the single $S_i^{n_i}$, each of which has a regular cycle by the induction hypothesis, and so A has a regular cycle by Lemma 2.2.6.
4. Case: G is not completely reducible. Set $B := \mathrm{Soc}(G)$, and note that B is proper in G and $\mathrm{C}_G(B) = \{1_G\}$. Denote by $\tilde{A}$ the periodic affine map of G/B induced by A, and let k denote the length of the identity element of G/B under $\tilde{A}$. Set $A_0 := A^k$. Then A_0 restricts to a periodic affine map of B, so by the induction hypothesis, $A_{0|B}$ has a cycle of length $n := \mathrm{ord}(A_{0|B})$; fix an element $x \in B$ such that $\mathrm{cl}_{A_0}(x) = n$. Now A_0^n acts identically in B, and thus by Lemma 2.2.5 also in $G \cong G/\mathrm{C}_G(B)$. This means that $n = \mathrm{ord}(A_0)$, and so $\mathrm{ord}(A) \leq k \cdot n$. But clearly, $\mathrm{cl}_A(x) = k \cdot n$, since k divides the cycle length under A of any element from B. Therefore, $\mathrm{ord}(A) = k \cdot n$ and A has a regular cycle.

□

Corollary 2.2.8. *(1) Let G be a finite semisimple group. Then:*
(i) $\Lambda(G) = \mathrm{mao}(G)$.
(ii) $\Lambda_{\mathrm{aff}}(G) = \mathrm{meo}(\mathrm{Hol}(G))$.
(2) Let R be a finite centerless CR-group. Then:
(i) $\Lambda(\mathrm{Aut}(R)) = \mathrm{mao}(R)$.
(ii) $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(R)) = \mathrm{meo}(\mathrm{Hol}(\mathrm{Aut}(R)))$.

Proof. For (1): (i) is an immediate consequence of Theorem 2.2.3, and (ii) also follows from Theorem 2.2.3 and the fact that $\mathrm{Aff}(G) \cong \mathrm{Hol}(G)$.

For (2): As for (i), note that $\mathrm{Aut}(R)$ is semisimple, and so by (1,i), we have $\Lambda(\mathrm{Aut}(R)) = \mathrm{mao}(\mathrm{Aut}(R)) = \mathrm{meo}(\mathrm{Aut}(\mathrm{Aut}(R))) = \mathrm{meo}(\mathrm{Aut}(R)) = \mathrm{mao}(R)$, where the second-to-last equality follows from the completeness of $\mathrm{Aut}(R)$. (ii) just is a special case of (1,ii). □

2.3 Upper bounds on element orders in wreath products

We will need upper bounds on $\mathrm{meo}(G)$ and $\mathrm{mao}(G)$ for finite semisimple groups G. To this end, some bounds on orders of elements in wreath products in general come in handy. Before formulating and proving Lemma 2.3.2 below, we introduce the following notation and terminology:

Definition 2.3.1. *Let G be a finite group, $n \in \mathbb{N}^+$, and $\psi \in \mathcal{S}_n$.*
(1) Let $g = (g_1, \ldots, g_n) \in G^n$. For $i = 1, \ldots, n$, we define $\mathrm{el}_i^{(\psi)}(g) := g_i g_{\psi^{-1}(i)} \cdots g_{\psi^{-\mathrm{cl}_\psi(i)+1}(i)} \in G$. Alternatively, one can describe $\mathrm{el}_i^{(\psi)}(g)$ as the image of $\mathrm{sh}_{\tau_\psi}^{(\mathrm{cl}_\psi(i))}(g) \in G^n \leq G \wr \mathcal{S}_n$ under the projection $\pi_i : G^n \to G$ onto the i-th component.
(2) We denote the set of orbits of the action of ψ on $\{1, \ldots, n\}$ by $\mathrm{Orb}(\psi)$.
(3) An ***assignment to ψ in G*** *is a function $\beta : \mathrm{Orb}(\psi) \to G$. For such an assignment β, we define its* ***order*** *to be the least common multiple of the numbers $\mathrm{ord}(\beta(O)^{\frac{\mathrm{ord}(\beta)}{|O|}})$, where O runs through $\mathrm{Orb}(\psi)$.*

Lemma 2.3.2. *Let G be a finite group, $n \in \mathbb{N}^+$, denote by $\pi : G \wr \mathcal{S}_n \to \mathcal{S}_n$ the canonical projection, and let $\psi \in \mathcal{S}_n$.*
(1) Let $g = (g_1, \ldots, g_n) \in G^n$ and consider the element $x := (g, \psi) \in G^n \rtimes \mathcal{S}_n = G \wr \mathcal{S}_n$. Then for $i = 1, \ldots, n$, the i-th component of $x^{\mathrm{ord}(\psi)} \in G^n$ equals $\mathrm{el}_i^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}}$.
(2) In particular, the maximum order of an element $x \in G \wr \mathcal{S}_n$ such that $\pi(x) = \psi$ equals the product of $\mathrm{ord}(\psi)$ with the maximum order of an assignment to ψ in G and is bounded from above by $\mathrm{ord}(\psi) \cdot \mathrm{meo}(G^{|\mathrm{Orb}(\psi)|})$.

Proof. For (1): We may assume that G is nontrivial. Fix i, and denote by $\pi_i : G^n \to G$ the projection onto the i-th component. It is clear that $x^{\mathrm{ord}(\psi)} = \mathrm{sh}_{\tau_\psi}(g)$ (where the shift is formed inside $G \wr \mathcal{S}_n$ and τ_ψ is the inner automorphism of $G \wr \mathcal{S}_n$ with respect to ψ), whence $\pi_i(x^{\mathrm{ord}(\psi)}) = \pi_i(\mathrm{sh}_{\tau_\psi}(g))$. But the i-th component of $\mathrm{sh}_{\tau_\psi}(g)$ only depends on the components of g whose indices are from the orbit O_i of i under ψ, so if we denote by $\tilde{g}$ the element of G^n which has the same entries as g in the components whose indices are in O_i but all other entries equal to 1_G, we have $\pi_i(x^{\mathrm{ord}(\psi)}) = \pi_i(\mathrm{sh}_{\tau_\psi}(\tilde{g}))$. Now note that $\mathrm{cl}_\psi(i)$ is a multiple of $\mathrm{cl}_{\tau_\psi}(\tilde{g})$ and a divisor of $\mathrm{ord}(\psi) = \mathrm{ord}(\tau_\psi)$, which gives us, by an application of Lemma 2.1.5(2),

$$\pi_i(x^{\mathrm{ord}(\psi)}) = \pi_i(\mathrm{sh}_{\tau_\psi}(\tilde{g})) = \pi_i(\mathrm{sh}_{\tau_\psi}^{(\mathrm{cl}_\psi(i))}(\tilde{g})^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}}) = \pi_i(\mathrm{sh}_{\tau_\psi}^{(\mathrm{cl}_\psi(i))}(\tilde{g}))^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}} =$$

$$\pi_i(\mathrm{sh}_{\tau_\psi}^{(\mathrm{cl}_\psi(i))}(g))^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}} = \mathrm{el}_i^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}}.$$

For (2): For any element $x \in G \wr \mathcal{S}_n$ of the form (g, ψ), we have $\mathrm{ord}(x) = \mathrm{ord}(\psi) \cdot \mathrm{ord}(x^{\mathrm{ord}(\psi)})$, where, by (1), the second factor is the least common multiple of the numbers $\mathrm{ord}(\mathrm{el}_i^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}})$ for $i = 1, \ldots, n$. Fix a set $\mathcal{R}$ of representatives of the orbits of ψ, which is in canonical bijection with $\mathrm{Orb}(\psi)$. It is not difficult to see that if $i, j \in \{1, \ldots, n\}$ are from the same orbit under ψ, then $\mathrm{el}_i^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(i)}}$ and $\mathrm{el}_j^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}_\psi(j)}}$ are conjugate in G and thus have the same order, so $\mathrm{ord}(x^{\mathrm{ord}(\psi)})$ is equal to just the least common multiple of the numbers $\mathrm{ord}(\mathrm{el}_i^{(\psi)}(g)^{\frac{\mathrm{ord}(\psi)}{\mathrm{cl}\,\psi(i)}})$ for $i \in \mathcal{R}$. Therefore, composing the canonical bijection $\mathrm{Orb}(\psi) \to \mathcal{R}$ with the function $\mathcal{R} \to G, i \mapsto \mathrm{el}_i^{(\psi)}(g)$ gives an assignment to ψ in G whose order coincides with $\mathrm{ord}(x^{\mathrm{ord}(\psi)})$. Conversely, if any assignment β to ψ in G is given, by choosing the components $g_1, \ldots, g_n$ of G such that for all $O \in \mathrm{Orb}(\psi)$ there exists $i \in O$ such that $g_i g_{\psi^{-1}(i)} \cdots g_{\psi^{-\mathrm{cl}_\psi(i)+1}(i)} = \beta(O)$, we can assure that $\mathrm{ord}((g, \psi)^{\mathrm{ord}(\psi)}) = \mathrm{ord}(\beta)$. This proves the claim. □

2.4 Landau's and Chebyshev's function

Both Landau's function $g : \mathbb{N}^+ \to \mathbb{N}^+, n \mapsto \mathrm{meo}(\mathcal{S}_n)$, and Chebyshev's function $\psi : \mathbb{N}^+ \to \mathbb{N}^+, n \mapsto \log(\exp(\mathcal{S}_n))$, are well-studied in analytic number theory. Apart from information on their asymptotic growth behavior, explicit upper bounds are also available. More explicitly, Massias [8, Théorème, p. 271] proved that $\log(g(n)) \leq 1.05314 \cdot \sqrt{n \log(n)}$ for all $n \in \mathbb{N}^+$, and Rosser and Schoenfeld [11, Theorem 12] that $\psi(n) < 1.03883 \cdot n$ for all $n \in \mathbb{N}^+$.

The latter result translates into an exponential upper bound on $\Psi := \exp \circ \psi$. For $n \leq 27$, the following best possible exponential bound on $g(n)$ is sharper than the subexponential bound by Massias, and its use will make some of our arguments easier:

Proposition 2.4.1. *For all $n \in \mathbb{N}^+$, we have $g(n) \leq 3^{\frac{n}{3}}$, with equality if and only if $n = 3$.* □

We conclude with the following consequence of Lemma 2.3.2:

Lemma 2.4.2. *(1) Let G be a finite group, $n \in \mathbb{N}+$. Then $\mathrm{meo}(G \wr \mathcal{S}_n) \leq g(n) \cdot \mathrm{meo}(G^n)$.*
(2) Let S be a nonabelian finite simple group, $n \in \mathbb{N}$. Then $g(n) \cdot \mathrm{meo}(\mathrm{Aut}(S)^n) < |S|^{n/3}$ implies that $\Lambda(\mathrm{Aut}(S^n)) < |S^n|^{1/3}$ and $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(S^n)) < |S^n|^{2/3}$.

Proof. For (1): This follows immediately from Lemma 2.3.2(2).
For (2): Using Corollary 2.2.8(2), we conclude that $\Lambda(\mathrm{Aut}(S^n)) = \mathrm{meo}(\mathrm{Aut}(S^n)) = \mathrm{meo}(\mathrm{Aut}(S) \wr \mathcal{S}_n) \leq g(n) \cdot \mathrm{meo}(\mathrm{Aut}(S)^n) < |S|^{n/3} = |S^n|^{1/3}$, and that $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(S^n)) = \mathrm{meo}(\mathrm{Hol}(\mathrm{Aut}(S^n))) = \mathrm{meo}(\mathrm{Aut}(S^n) \rtimes \mathrm{Aut}(\mathrm{Aut}(S^n))) \leq \mathrm{meo}(\mathrm{Aut}(S^n)) \cdot \mathrm{meo}(\mathrm{Aut}(\mathrm{Aut}(S^n))) = \mathrm{meo}(\mathrm{Aut}(S^n))^2 < |S^n|^{2/3}$. □

3 Reduction to the main lemma

The aforementioned "main lemma" is the following:

Lemma 3.1. *Let G be a finite nonabelian characteristically simple group. Then:*
(1) $\Lambda(\mathrm{Aut}(G)) < |G|^{\frac{1}{3}}$, with the following exceptions:

(i) $G \cong \mathrm{PSL}_2(q)$ for some primary $q \geq 5$. In this case, $\Lambda(\mathrm{Aut}(G)) = q+1$, we have $\frac{1}{3} < \log_{|G|}(q+1) \leq \frac{\log(q+1)}{\log(\frac{1}{2}q(q^2-1))}$, and for $q \to \infty$, this upper bound converges to $\frac{1}{3}$ strictly monotonously from above.

(ii) $G \cong \mathrm{PSL}_2(p)^2$ for some prime $p \geq 5$. In this case, $\Lambda(\mathrm{Aut}(G)) = p(p+1)$, we have $\frac{1}{3} < \log_{|G|}(p(p+1)) = \frac{\log(p(p+1))}{\log(\frac{1}{2}p(p^2-1))}$, and for $p \to \infty$, this upper bound converges to $\frac{1}{3}$ strictly monotonously from above.

(iii) $G \cong \mathrm{PSL}_2(p)^3$ for some prime $p \geq 5$. In this case, $\Lambda(\mathrm{Aut}(G)) = \frac{1}{2}p(p^2-1) = |G|^{\frac{1}{3}}$.

(2) $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(G)) \leq |G|^{\frac{2}{3}}$, with the following exceptions: $G \cong \mathrm{PSL}_2(p)$ for some prime $p \geq 5$. In this case, $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(G)) = p(p+1)$, we have $\frac{2}{3} < \log_{|G|}(p(p+1)) = \frac{\log(p(p+1))}{\log(\frac{1}{2}p(p^2-1))}$, and for $p \to \infty$, this upper bound converges to $\frac{2}{3}$ strictly monotonously from above.

The purpose of this section is to show how to deduce all the main results from Lemma 3.1, so until the end of this section, the word "proof" means "proof conditional on Lemma 3.1". We first give the precise definition of the constants E_1 and E_2 from Theorem 1.1.1:

Notation 3.2. *(1) We set $e_1 := \log_{60}(6) = 0.437618\ldots$ and $E_1 := \frac{1}{e_1-1} = -1.778151\ldots$.*
(2) We set $e_2 := \log_{60}(30)$ and $E_2 := \frac{1}{e_2-1} = -5.906890\ldots$.

Lemma 3.3. *(1) For all finite nonabelian characteristically simple groups G, we have $\Lambda(\mathrm{Aut}(G)) \leq |G|^{e_1}$, with equality if and only if $G \cong \mathrm{PSL}_2(5) \cong \mathcal{A}_5$.*
(2) For every $\epsilon > 0$, we have $\Lambda(\mathrm{Aut}(G)) \leq |G|^{\frac{1}{3}+\epsilon}$ for almost all finite nonabelian characteristically simple groups G.
(3) For all finite nonabelian characteristically simple groups G, we have $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(G)) \leq |G|^{e_2}$, with equality if and only if $G \cong \mathrm{PSL}_2(5) \cong \mathcal{A}_5$.
(4) For every $\epsilon > 0$, we have $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(G)) \leq |G|^{\frac{2}{3}+\epsilon}$ for almost all finite nonabelian characteristically simple groups G.

Proof. The statements in (2) and (4) follow immediately from Lemma 3.1. For (1), note that by Lemma 3.1(1), we have $\Lambda(\mathrm{Aut}(\mathrm{PSL}_2(5))) = 6 = |\mathrm{PSL}_2(5)|^{e_1}$, and using the strict monotonicity of the upper bounds in Lemma 3.1(1), it is not difficult to see that this is the only case where equality holds. The proof of (2) is analogous. □

Lemma 3.4. *Let H be a finite semisimple group. Then:*
(1) $\Lambda(H) \leq |\mathrm{Soc}(H)|^{e_1}$.
(2) $\Lambda_{\mathrm{aff}}(H) \leq |\mathrm{Soc}(H)|^{e_2}$.

Proof. Let $S_1, \ldots, S_r$ be pairwise nonisomorphic nonabelian finite simple groups, $n_1, \ldots, n_r \in \mathbb{N}^+$ such that $\mathrm{Soc}(H) \cong S_1^{n_1} \times \cdots \times S_r^{n_r}$. Using the facts that $\mathrm{Aut}(H)$ embeds into $\mathrm{Aut}(\mathrm{Soc}(H))$, that $\Lambda(G) = \mathrm{meo}(\mathrm{Aut}(G))$ for all finite semisimple groups G (Corollary 2.2.8(1,i)) and that $\Lambda(R) = \mathrm{meo}(\mathrm{Aut}(R)) = \Lambda(\mathrm{Aut}(R))$ for all finite centerless CR-groups R (Corollary 2.2.8(1,i) and (2,i)), we conclude that

$$\Lambda(H) = \mathrm{meo}(\mathrm{Aut}(H)) \leq \mathrm{meo}(\mathrm{Aut}(\mathrm{Soc}(H))) = \Lambda(\mathrm{Soc}(H)) = \Lambda(S_1^{n_1} \times \cdots \times S_r^{n_r}) \leq$$

$$\leq \Lambda(S_1^{n_1}) \cdots \Lambda(S_r^{n_r}) = \Lambda(\mathrm{Aut}(S_1^{n_1})) \cdots \Lambda(\mathrm{Aut}(S_r^{n_r})) \leq |S_1|^{e_1 n_1} \cdots |S_r|^{e_1 n_r} = |\mathrm{Soc}(H)|^{e_1},$$

where the last inequality follows from Lemma 3.3(1). This proves the inequality in (1). For (2), we use the fact that H embeds into $\mathrm{Aut}(\mathrm{Soc}(H))$, that $\Lambda_{\mathrm{aff}}(G) = \mathrm{meo}(\mathrm{Hol}(G))$ for all finite semisimple groups G (Corollary 2.2.8(1,ii)) and that, by completeness of $\mathrm{Aut}(S_1^{n_1} \times \cdots \times S_r^{n_r}) = \mathrm{Aut}(S_1^{n_1}) \times \cdots \times \mathrm{Aut}(S_r^{n_r})$, the tuple $(\mathrm{Aut}(S_1^{n_1}), \ldots, \mathrm{Aut}(S_r^{n_r}))$ has the splitting property, to conclude, with one application of Lemma 3.3(3) at the end, that

$$\Lambda_{\mathrm{aff}}(H) = \mathrm{meo}(\mathrm{Hol}(H)) \leq \mathrm{meo}(\mathrm{Hol}(\mathrm{Aut}(\mathrm{Soc}(H)))) = \Lambda_{\mathrm{aff}}(\mathrm{Aut}(\mathrm{Soc}(H))) =$$

$$= \Lambda_{\mathrm{aff}}(\mathrm{Aut}(S_1^{n_1}) \times \cdots \times \mathrm{Aut}(S_r^{n_r})) \leq \Lambda_{\mathrm{aff}}(\mathrm{Aut}(S_1^{n_1})) \cdots \Lambda_{\mathrm{aff}}(\mathrm{Aut}(S_r^{n_r})) \leq$$

$$\leq |S_1|^{e_2 n_1} \cdots |S_r|^{e_2 n_r} = |\mathrm{Soc}(H)|^{e_2}.$$

□

Proof of Theorem 1.1.1. For (1), using the assumption as well as Lemmata 2.1.3(1) and 3.4(1), we conclude that $\rho \leq \lambda(G) \leq \lambda_{\mathrm{aff}}(\mathrm{Rad}(G)) \cdot \lambda(G/\mathrm{Rad}(G)) \leq 1 \cdot |G/\mathrm{Rad}(G)|^{e_1-1}$, and so $[G : \mathrm{Rad}(G)] \geq \rho^{\frac{1}{e_1-1}}$. The proof for (2) is analogous. □

Proof of Corollary 1.1.2. The statements about cycle lengths in $\mathcal{A}_5 \cong \mathrm{PSL}_2(5)$ follow immediately from Lemma 3.1. As for the two asserted implications:
For (1): By Theorem 1.1.1(1) (and strict monotonicity of power functions), $\lambda(G) > \frac{1}{10}$ implies that $[G : \mathrm{Rad}(G)] < (\frac{1}{10})^{E_1} = 60$, and thus that $[G : \mathrm{Rad}(G)] = 1$.
For (2): This is similar to (1), but more involved. By Theorem 1.1.1(2), $\lambda_{\mathrm{aff}}(G) > \frac{1}{4}$ implies that $[G : \mathrm{Rad}(G)] < (\frac{1}{4})^{E_2} = 3600$. So if any nonsolvable finite group G with $\lambda_{\mathrm{aff}}(G) > \frac{1}{4}$ existed, then $G/\mathrm{Rad}(G)$ would have socle a nonabelian finite simple group S of order less than 3600. By Lemma 2.1.3(2), it would follow that $\lambda_{\mathrm{aff}}(S) > \frac{1}{4}$, so in order to get a contradiction, it suffices to check that $\lambda_{\mathrm{aff}}(S) \leq \frac{1}{4}$ for all nonabelian finite simple groups S such that $|S| < 3600$. By CFSG, there are precisely eight such S, namely $\mathrm{PSL}_2(q)$ for $q = 5, 7, 9, 8, 11, 13, 17$ and $\mathcal{A}_7$. By Corollary 2.2.8(1,ii), it is sufficient to compute $\frac{\mathrm{meo}(\mathrm{Hol}(S))}{|S|}$ for these eight S, which we did with the help of GAP [3]. For the $\mathrm{PSL}_2(q)$, the results are summarized in Table 1, and we also got that $\lambda_{\mathrm{aff}}(\mathcal{A}_7) = \frac{1}{42}$:

Table 1: λ_{aff}-values of the nonabelian finite simple groups of order smaller than 3600, excluding $\mathcal{A}_7$

q	5	7	9	8	11	13	17
$\lambda_{\mathrm{aff}}(\mathrm{PSL}_2(q))$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{9}$	$\frac{1}{8}$	$\frac{1}{10}$	$\frac{1}{12}$	$\frac{1}{16}$

□

For proving Theorem 1.1.3, we introduce the following notation:

Notation 3.5. *(1) For $\kappa \in \left(0, \frac{2}{3}\right]$ and $\kappa_{\mathrm{aff}} \in \left(0, \frac{1}{3}\right]$, we denote by $\mathcal{T}^{(\kappa)}$ the set of finite nonabelian characteristically simple groups T such that $\Lambda(\mathrm{Aut}(T)) \geq |T|^{\frac{1}{3}+\kappa}$, and by $\mathcal{T}_{\mathrm{aff}}^{(\kappa_{\mathrm{aff}})}$ the set of finite nonabelian characteristically simple groups T such that $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(T)) \geq |T|^{\frac{2}{3}+\kappa_{\mathrm{aff}}}$. Note that by Lemma 3.1, $\mathcal{T}^{(\kappa)}$ and $\mathcal{T}_{\mathrm{aff}}^{(\kappa_{\mathrm{aff}})}$ are finite.*
(2) For $\epsilon \in \left(0, \frac{2}{3}\right]$, $\epsilon_{\mathrm{aff}} \in \left(0, \frac{1}{3}\right]$ and $\rho \in (0,1)$, set

$$C^{(1)}(\epsilon,\rho) := \prod_{T \in \mathcal{T}^{(\rho\epsilon)}} \frac{\Lambda(\mathrm{Aut}(T))}{|T|^{\frac{1}{3}+\rho\epsilon}} \text{ and } C_{\mathrm{aff}}^{(1)}(\epsilon_{\mathrm{aff}},\rho) := \prod_{T \in \mathcal{T}_{\mathrm{aff}}^{(\rho\epsilon_{\mathrm{aff}})}} \frac{\Lambda_{\mathrm{aff}}(\mathrm{Aut}(T))}{|T|^{\frac{2}{3}+\rho\epsilon_{\mathrm{aff}}}},$$

$$C^{(2)}(\epsilon,\rho) := \prod_{T \in \mathcal{T}^{(\frac{1}{2}\rho\epsilon)}} |T| \text{ and } C_{\mathrm{aff}}^{(2)}(\epsilon_{\mathrm{aff}},\rho) := \prod_{T \in \mathcal{T}_{\mathrm{aff}}^{(\frac{1}{2}\rho\epsilon_{\mathrm{aff}})}} |T|,$$

$$C(\epsilon,\rho) := C^{(1)}(\epsilon,\rho)^{\frac{1}{\rho/2\cdot\epsilon}} \cdot C^{(2)}(\epsilon,\rho) \text{ and } C_{\mathrm{aff}}(\epsilon_{\mathrm{aff}},\rho) := C_{\mathrm{aff}}^{(1)}(\epsilon_{\mathrm{aff}},\rho)^{\frac{1}{\rho/2\cdot\epsilon_{\mathrm{aff}}}} \cdot C_{\mathrm{aff}}^{(2)}(\epsilon_{\mathrm{aff}},\rho),$$

$$D(\epsilon,\rho) := \max\{|H|+1 \mid H \text{ a finite semisimple group such that } |\mathrm{Soc}(H)| < C(\epsilon,\rho)\},$$

and

$$D_{\mathrm{aff}}(\epsilon_{\mathrm{aff}},\rho) := \max\{|H|+1 \mid H \text{ a finite semisimple group such that } |\mathrm{Soc}(H)| < C_{\mathrm{aff}}(\epsilon_{\mathrm{aff}},\rho)\}.$$

Theorem 1.1.3(1) will follow rather easily from the following:

Theorem 3.6. *Let $\epsilon \in \left(0, \frac{2}{3}\right], \epsilon_{\mathrm{aff}} \in \left(0, \frac{1}{3}\right], \rho \in (0,1)$.*
(1) Let H be a finite semisimple group such that $|H| \geq D(\epsilon,\rho)$ holds. Then $\Lambda(H) \leq |\operatorname{Soc}(H)|^{\frac{1}{3}+\rho\epsilon}$.
(2) Let H be a finite semisimple group such that $|H| \geq D_{\mathrm{aff}}(\epsilon_{\mathrm{aff}},\rho)$ holds. Then $\Lambda_{\mathrm{aff}}(H) \leq |\operatorname{Soc}(H)|^{\frac{2}{3}+\rho\epsilon_{\mathrm{aff}}}$.
(3) Let G be a finite group such that $\Lambda(G) \geq |G|^{\frac{1}{3}+\epsilon}$. Then we have the following: $[G:\operatorname{Rad}(G)] \leq \max(D(\epsilon,\rho), |G|^{\frac{2/3-\epsilon}{2/3-\rho\epsilon}})$.
(4) Let G be a finite group such that $\Lambda_{\mathrm{aff}}(G) \geq |G|^{\frac{2}{3}+\epsilon_{\mathrm{aff}}}$. Then we have the following: $[G:\operatorname{Rad}(G)] \leq \max(D_{\mathrm{aff}}(\epsilon_{\mathrm{aff}},\rho), |G|^{\frac{1/3-\epsilon_{\mathrm{aff}}}{1/3-\rho\epsilon_{\mathrm{aff}}}})$.

Proof. For (1): Let $S_1,\ldots,S_r$ be pairwise nonisomorphic nonabelian finite simple groups and $n_1,\ldots,n_r \in \mathbb{N}^+$ such that $\operatorname{Soc}(H) \cong S_1^{n_1} \times \cdots \times S_r^{n_r}$. For $i=1,\ldots,r$, set $T_i := S_i^{n_i}$. Note that, as in the proof of Lemma 3.4(1), we have $\Lambda(H) \leq \Lambda(\operatorname{Aut}(T_1)) \cdots \Lambda(\operatorname{Aut}(T_r))$.

The idea is the following: We will bound each $\Lambda(\operatorname{Aut}(T_i))$ from above by a power $|T_i|^{f_i}$, and we would be done if all f_i were less than or equal to $\frac{1}{3}+\rho\epsilon$. In view of the exceptional cases in Lemma 3.1, we cannot expect this to happen, but since by the same lemma, almost all finite nonabelian characteristically simple T satisfy $\Lambda(\operatorname{Aut}(T)) < |T|^{\frac{1}{3}+\frac{\rho\epsilon}{2}}$, and this upper bound has some capacity to "swallow" factors greater than 1 and still remain smaller than $|T|^{\frac{1}{3}+\rho\epsilon}$, if the order of $|\operatorname{Soc}(H)|$ is large enough, the "swallowing capacity" of the factors $T_i \notin \mathcal{T}^{(\frac{\rho\epsilon}{2})}$ will be big enough to make up for the "spillover" of all "problematic" factors coming from the finite set $\mathcal{T}^{(\rho\epsilon)}$.

Formally, we proceed as follows. W.l.o.g., assume that there exist $k,l \in \mathbb{N}$ with $k+l \leq r$ such that $T_1,\ldots,T_k \in \mathcal{T}^{(\rho\epsilon)}$, $T_{k+1},\ldots,T_{k+l} \in \mathcal{T}^{(\frac{1}{2}\rho\epsilon)} \setminus \mathcal{T}^{(\rho\epsilon)}$ and $T_{k+l+1},\ldots,T_r \notin \mathcal{T}^{(\frac{1}{2}\rho\epsilon)}$. Note that by definition of $D(\epsilon,\rho)$ and the assumption, we have $|\operatorname{Soc}(H)| \geq C(\epsilon,\rho)$. By definition of $C_2(\epsilon,\rho)$, we have $|T_1|\cdots|T_{k+l}| \leq C_2(\epsilon,\rho)$, and so by definition of $C(\epsilon,\rho)$, we conclude that $|T_{k+l+1}|\cdots|T_r| = \frac{|\operatorname{Soc}(H)|}{|T_1|\cdots|T_{k+l}|} \geq \frac{C(\epsilon,\rho)}{C_2(\epsilon,\rho)} = C_1(\epsilon,\rho)^{\frac{1}{\rho/2\cdot\epsilon}}$. It follows that

$$\Lambda(H) \leq \prod_{i=1}^{k} \Lambda(\operatorname{Aut}(T_i)) \cdot \prod_{i=k+1}^{k+l} \Lambda(\operatorname{Aut}(T_i)) \cdot \prod_{i=k+l+1}^{r} \Lambda(\operatorname{Aut}(T_i)) \leq$$

$$\leq \prod_{i=1}^{k} |T_i|^{\frac{1}{3}+\rho\epsilon} \cdot C_1(\epsilon,\rho) \cdot \prod_{i=k+1}^{k+l} |T_i|^{\frac{1}{3}+\rho\epsilon} \cdot \prod_{i=k+l+1}^{r} |T_i|^{\frac{1}{3}+\rho\epsilon} \cdot (\prod_{i=k+l+1}^{r} |T_i|)^{-\frac{\rho\epsilon}{2}} \leq$$

$$\leq |\operatorname{Soc}(H)|^{\frac{1}{3}+\rho\epsilon} \cdot C_1(\epsilon,\rho) \cdot (C_1(\epsilon,\rho)^{\frac{1}{\rho/2\cdot\epsilon}})^{-\frac{\rho\epsilon}{2}} = |\operatorname{Soc}(H)|^{\frac{1}{3}+\rho\epsilon}.$$

For (2): This is analogous to the proof of (1).
For (3): We show the contraposition: Assume that G is a finite group such that $[G:\operatorname{Rad}(G)] > \max(D(\epsilon,\rho), |G|^{\frac{2/3-\epsilon}{2/3-\rho\epsilon}})$. We need to show that $\Lambda(G) < |G|^{\frac{1}{3}+\epsilon}$. Note that by (1), we have $\Lambda(G/\operatorname{Rad}(G)) \leq |\operatorname{Soc}(G/\operatorname{Rad}(G))|^{\frac{1}{3}+\rho\epsilon} \leq |G/\operatorname{Rad}(G)|^{\frac{1}{3}+\rho\epsilon}$. It follows that

$$\Lambda(G) \leq \Lambda_{\mathrm{aff}}(\operatorname{Rad}(G)) \cdot \Lambda(G/\operatorname{Rad}(G)) \leq |\operatorname{Rad}(G)| \cdot |G/\operatorname{Rad}(G)|^{\frac{1}{3}+\rho\epsilon} =$$

$$= |\operatorname{Rad}(G)|^{\frac{2}{3}-\rho\epsilon} \cdot |G|^{\frac{1}{3}+\rho\epsilon} < (|G|^{1-\frac{2/3-\epsilon}{2/3-\rho\epsilon}})^{\frac{2}{3}-\rho\epsilon} \cdot |G|^{\frac{1}{3}+\rho\epsilon} = |G|^{\epsilon-\rho\epsilon} \cdot |G|^{\frac{1}{3}+\rho\epsilon} = |G|^{\frac{1}{3}+\epsilon}.$$

For (4): This is analogous to the proof of (3). □

Proof of Theorem 1.1.3. For (1): Set $K(\epsilon,\xi) := D(\epsilon, \frac{2/3\xi}{\epsilon(1-3/2\epsilon+\xi)})$. Then by setting $\rho := \frac{2/3\xi}{\epsilon(1-3/2\epsilon+\xi)}$ in Theorem 3.6(2), we find that $\Lambda(G) \geq |G|^{\frac{1}{3}+\epsilon}$ implies

$$[G:\operatorname{Rad}(G)] \leq \max(D(\epsilon,\rho), |G|^{\frac{2/3-\epsilon}{2/3-\rho\epsilon}}) = \max(K(\epsilon,\xi), |G|^{1-3/2\epsilon+\xi}).$$

For (2): This is analogous to (1).
For (3): Denote by p_n the n-th prime number (starting with $p_0 = 2$) and set $G_n := \operatorname{PGL}_2(p_{n+2}) = \operatorname{Aut}(\operatorname{PSL}_2(p_{n+2}))$. That this choice of G_n does the job follows from Lemma 3.1, since $\log_{p(p^2-1)}(p+1) > \frac{1}{3}$ and $\log_{p(p^2-1)}(p(p+1)) > \frac{2}{3}$ for all primes $p \geq 5$. □

4 Proof of the main lemma

We now tackle the final task of proving the main lemma, Lemma 3.1. So let $G = S^n$, where S is a nonabelian finite simple group and $n \in \mathbb{N}^+$. We make a case-by-case analysis using the CFSG. In most cases, Lemma 2.4.2(2) will be sufficient to this end, but some cases require sharper upper bounds.

4.1 Case: S is sporadic

Using Lemma 2.4.2(2) and the information on $|S|, \mathrm{Out}(S)$ and $\mathrm{meo}(S)$ for sporadic S from [2], this case only consists in some routine checks.

4.2 Case: $S = \mathcal{A}_m, m \geq 7$

Note that $\mathcal{A}_5 \cong \mathrm{PSL}_2(5)$ and $\mathcal{A}_6 \cong \mathrm{PSL}_2(9)$ will be treated in the next case. We also use Lemma 2.4.2(2) here. That is, we want to show that $g(n) \cdot \mathrm{meo}(\mathcal{S}_m^n) < (\frac{1}{2}m!)^{n/3}$ for all $n \in \mathbb{N}^+$ and all $m \geq 7$.

For $n = 1$, this is the inequality $g(m) < (\frac{1}{2}m!)^{1/3}$ for $m \geq 7$. But $g(m) < 3^{m/3}$, and one easily verifies $3^{m/3} < (\frac{1}{2}m!)^{1/3}$ for all $m \geq 7$.

For $n = 2$, the inequality turns into $2 \cdot \mathrm{meo}(\mathcal{S}_m^2) < (\frac{1}{2}m!)^{2/3}$. Now $\mathrm{meo}(\mathcal{S}_m^2) < g(m)^2$, and it is easy to verify $2 \cdot g(m)^2 < (\frac{1}{2}m!)^{2/3}$ for $m \geq 7$.

For $n = 3$, the inequality to show is $3 \cdot \mathrm{meo}(\mathcal{S}_m^3) < \frac{1}{2}m!$, and it is easy to verify the stronger $3 \cdot g(m)^3 < \frac{1}{2}m!$.

Finally, for $n \geq 4$, we use the bound $g(n) \cdot \mathrm{meo}(\mathcal{S}_m^n) < 3^{n/3} \cdot \Psi(m) < 3^{n/3} \cdot \mathrm{e}^{1.03883 \cdot m}$, which reduces the inequality to $\mathrm{e}^{1.03883 \cdot m} < (\frac{1}{6}m!)^{n/3}$ for $n \geq 4$ and $m \geq 7$, and this is easy to verify.

4.3 Case: $S = \mathrm{PSL}_2(q), q \geq 5$

This is the most complicated case, requiring to investigate the five subcases $n = 1, 2, 3, 4$ and $n \geq 5$. Recall that $\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, and in particular, there is a natural embedding $\mathrm{PSL}_2(q) \hookrightarrow \mathrm{PGL}_2(q)$.

4.3.1 Subcase: $n = 1$

Our goal is to show the following:

Theorem 4.3.1.1. *Let $q \geq 5$ be primary. Then:*
(1) $\Lambda(\mathrm{Aut}(\mathrm{PSL}_2(q))) = q + 1$.

$$(2)\ \Lambda_{\mathrm{aff}}(\mathrm{Aut}(\mathrm{PSL}_2(q))) = \begin{cases} q(q+1), & \textit{if } q \textit{ is prime}, \\ q^2 - 1, & \textit{if } q \textit{ is even}, \\ \frac{1}{2}(q^2-1), & \textit{if } q \textit{ is odd and not prime}. \end{cases}.$$

By Corollary 2.2.8(2,i), $\Lambda(\mathrm{Aut}(\mathrm{PSL}_2(q))) = \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)))$, which was already determined by Guest, Morris, Praeger and Spiga in [5], see Table 3 there. The following lemma is an extract from the proof of [5, Theorem 2.16]:

Lemma 4.3.1.2. *Let $q \geq 5$ be primary, with prime base p.*
(1) Denote by $\pi : \mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ *the canonical projection. Let* $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ *such that* $\mathrm{ord}(\pi(\alpha)) = e$. *Then* $\mathrm{ord}(\alpha) \leq e \cdot (q^{1/e} + 1)$.
(2) $\mathrm{mao}(\mathrm{PSL}_2(q)) = q + 1$. □

They proved point (2) using point (1) (whose proof used Lang-Steinberg maps). Since point (1) of Theorem 4.3.1.1 is now clear, let us outline the strategy for proving point (2): By Theorem 2.2.3, we know that the largest cycle length of any periodic affine map $\mathrm{A}_{x,\alpha}$ of $\mathrm{Aut}(\mathrm{PSL}_2(q))$ coincides with its order, which is the product $\mathrm{ord}(\alpha) \cdot \mathrm{ord}(\mathrm{sh}_\alpha(x))$. By completeness of $\mathrm{Aut}(\mathrm{PSL}_2(q))$, we know that $\mathrm{ord}(\alpha)$ is an element order in $\mathrm{Aut}(\mathrm{PSL}_2(q))$, so the order of any periodic affine map of

$\mathrm{Aut}(\mathrm{PSL}_2(q))$ is the product of two automorphism orders of $\mathrm{PSL}_2(q)$. If we know a list of the first few largest automorphism orders of $\mathrm{PSL}_2(q)$ which is long enough to ensure that for any periodic affine map whose order exceeds the asserted Λ_{aff}-value, the two factor orders must be in the list, we can systematically go through the possible combinations, deriving a contradiction in each case using Lemmata 2.1.6 and 2.1.7. It will then remain to show that the asserted Λ_{aff}-value is indeed the Λ-value of some periodic affine map of $\mathrm{Aut}(\mathrm{PSL}_2(q))$, which can be done by Lemma 2.1.8.

We can indeed extend the list of largest automorphism orders of $\mathrm{PSL}_2(q)$ to our needs in a way similar to how Guest, Morris, Praeger and Spiga derived point (2) of Lemma 4.3.1.2 from point (1):

Lemma 4.3.1.3. *(1) Let $q = 2^f$ with $f \geq 3$. The two largest automorphism orders of $\mathrm{PSL}_2(q)$ are $q+1$ and $q-1$.*
(2) Let $q = p^f \geq 5$ with p an odd prime and $f \geq 1$.
(i) If $f = 1$, then the five largest automorphism orders of $\mathrm{PSL}_2(q)$ are $q+1, q, q-1, \frac{q+1}{2}, \frac{q-1}{2}$.
(ii) If $f \geq 2$ and $(p, f) \neq (3, 2)$, then the four largest automorphism orders of $\mathrm{PSL}_2(q)$ are $q+1, q-1, \frac{q+1}{2}, \frac{q-1}{2}$. Also, $\mathrm{ord}(\alpha) \leq \frac{q-1}{2}$ for any $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q)) \setminus \mathrm{PGL}_2(q)$, where the inequality is strict for $q \neq 25$.
(iii) The four largest automorphism orders of $\mathrm{PSL}_2(9) \cong \mathcal{A}_6$ are $10, 8, 6, 5$.

For those parts of the argument where we will use Lemma 2.1.7, we will need some statements about centralizers in $\mathrm{Aut}(\mathrm{PSL}_2(q))$ for odd q:

Lemma 4.3.1.4. *(1) Let $p \geq 5$ be prime, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(p)) = \mathrm{PGL}_2(p)$ be of order p. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(p))}(\alpha) = \langle\alpha\rangle \subseteq \mathrm{PSL}_2(p)$.*
(2) Let $q \geq 5$ be odd, primary, $q \notin \{9, 25\}$, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ be of order $\frac{q-1}{2}$. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) \subseteq \mathrm{PGL}_2(q)$.
(3) Let $q \geq 5$ be odd, primary, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ be of order $q-1$. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) \subseteq \mathrm{PGL}_2(q)$.
(4) Let $q \geq 5$ be odd, primary, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ be of order $\frac{q+1}{2}$. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) \subseteq \mathrm{PGL}_2(q)$.
(5) Let $q \geq 5$ be odd, primary, and let $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(q))$ be of order $q+1$. Then $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) \subseteq \mathrm{PGL}_2(q)$.

Before proving Lemmata 4.3.1.3 and 4.3.1.4, for the readers' convenience, we quickly recall some basic facts on the element structure of $\mathrm{PGL}_2(q)$ for primary q with prime base p. We denote by $\pi_0 : \mathrm{GL}_2(q) \to \mathrm{PGL}_2(q)$ and $\pi_1 : \mathrm{GL}_2(q^2) \to \mathrm{PGL}_2(q^2)$ the canonical projections.

1. Every element order in $\mathrm{PGL}_2(q)$ is a divisor of one of the following: $p, q+1, q-1$.
2. Every element in $\mathrm{PGL}_2(q)$ of order p is conjugate in $\mathrm{PGL}_2(q)$ to an element of the form $\pi_0(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix})$ with $x \in \mathbb{F}_q^*$. These elements are also in $\mathrm{PSL}_2(q)$.
3. Every element in $\mathrm{PGL}_2(q)$ of order a divisor of $q-1$ is conjugate in $\mathrm{PGL}_2(q)$ to an element of the form $\pi_0(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix})$ with $a \in \mathbb{F}_q^*$. Clearly, the order of such an element in $\mathrm{PGL}_2(q)$ equals the order of $a \in \mathbb{F}_q^*$, so all divisors of $q-1$ occur as element orders. Furthermore, such an element is in $\mathrm{PSL}_2(q)$ if and only if a is a square in $\mathbb{F}_q$, whence for even q, all these elements are also in $\mathrm{PSL}_2(q)$, and for odd q, precisely those whose order is a divisor of $\frac{q+1}{2}$ are in $\mathrm{PSL}_2(q)$.
4. Every element in $\mathrm{PGL}_2(q)$ of order a divisor of $q+1$, but not of $q-1$, is conjugate in $\mathrm{PGL}_2(q^2)$ to an element of the form $\pi_1(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix})$ with $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. As before, all such divisors of $q+1$ occur as element orders, and among such elements, precisely those where a is a square in $\mathbb{F}_{q^2}$ are in $\mathrm{PSL}_2(q)$, so again, for even q, all such elements are also in $\mathrm{PSL}_2(q)$, and for odd q, precisely those whose order is a divisor of $\frac{q+1}{2}$ are also in $\mathrm{PSL}_2(q)$.

Proof of Lemma 4.3.1.3. Denote by $\pi:\mathrm{Aut}(\mathrm{PSL}_2(q))\to\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ the canonical projection.
For (1): That $q+1$ is the largest automorphism order is just a special case of Lemma 4.3.1.2(2), and $q-1$ is an automorphism order by the above facts on the element structure of $\mathrm{PGL}_2(q)$. It remains to show that $q=2^f$ is not an automorphism order, which goes as follows: If $\alpha\in\mathrm{Aut}(\mathrm{PSL}_2(q))$ had order 2^f, then $2^f=\mathrm{ord}(\alpha)=\mathrm{ord}(\pi(\alpha))\cdot\mathrm{ord}(\alpha^{\mathrm{ord}(\pi(\alpha))})$. Now by the element structure, the only element orders in $\mathrm{PGL}_2(q)$ which are powers of 2 are 1 and 2, and so $\mathrm{ord}(\alpha^{\mathrm{ord}(\pi(\alpha))})\leq 2$, and thus $\mathrm{ord}(\pi(\alpha))\geq 2^{f-1}$. But $\mathrm{ord}(\pi(\alpha))\mid|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_2)|=f$, a contradiction.
For (2,i): Since $\mathrm{Aut}(\mathrm{PSL}_2(q))=\mathrm{PGL}_2(q)$ if q is prime, the statement follows from the element structure of $\mathrm{PGL}_2(q)$.
For (2,ii): Again, by the element structure of $\mathrm{PGL}_2(q)$, the four listed numbers are certainly the four largest element orders in $\mathrm{PGL}_2(q)$, so it suffices to prove the second part of the claim. Let $\alpha\in\mathrm{Aut}(\mathrm{PSL}_2(q))\setminus\mathrm{PGL}_2(q)$, so that $e:=\mathrm{ord}(\pi(\alpha))>1$. We need to show that $\mathrm{ord}(\alpha)\leq\frac{q-1}{2}$, and actually $\mathrm{ord}(\alpha)<\frac{q-1}{2}$ unless $q=25$. By Lemma 4.3.1.2(1), it is sufficient to show that $e(q^{1/e}+1)<\frac{q-1}{2}$ for $q\neq 25$ (and to check that for $q=25$, where $e=2$, the left-hand side is equal to the right-hand side). For $q\neq 25$ (i.e., $q\geq 27$), note that it suffices to show

$$\frac{4}{3}eq^{1/e}\leq\frac{13}{27}q, \tag{1}$$

since

$$e(q^{1/e}+1)=eq^{1/e}(1+\frac{1}{q^{1/e}})\leq\frac{4}{3}eq^{1/e},$$

and

$$\frac{q-1}{2}=q(\frac{1}{2}-\frac{1}{2q})\geq q(\frac{1}{2}-\frac{1}{54})=\frac{13}{27}q.$$

(1) is equivalent to

$$q\geq(\frac{36}{13}e)^{1+\frac{1}{e-1}},$$

which is easy to verify in the case distinction $e=2$ (where $q\geq 49$) versus $e\geq 3$ (using that $q\geq 3^e$).
For (2,iii): This is readily checked with GAP [3]. □

We remark that, as is easy to check with GAP [3], $\mathrm{PSL}_2(25)$ actually has automorphisms of order $12=\frac{25-1}{2}$ that are not in $\mathrm{PGL}_2(25)$.

Proof of Lemma 4.3.1.4. For (1): By the element structure of $\mathrm{PGL}_2(p)$, we have $\alpha\in\mathrm{PSL}_2(p)$, and α is conjugate in $\mathrm{PGL}_2(p)$ to an element of the form $\pi_0(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix})$ for some $x\in\mathbb{F}_p^*$, so it suffices to prove the assertion for all such elements. However, since they are powers of one another, it actually suffices to show the assertion for $\alpha=\pi_0(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix})$. So let $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{GL}_2(p)$ such that

$$\pi_0(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix})=\pi_0(\begin{pmatrix}a & b\\ c & d\end{pmatrix}). \tag{2}$$

(2) is equivalent to the existence of some $\lambda\in\mathbb{F}_p^*$ such that

$$\begin{pmatrix}a+c & b+d-a-c\\ c & d-c\end{pmatrix}=\lambda\cdot\begin{pmatrix}a & b\\ c & d\end{pmatrix}. \tag{3}$$

If $\lambda\neq 1$, then a comparison of the bottom left entries in (3) implies $c=0$ and thus also $a=0$, a contradiction. So $\lambda=1$, turning (3) into a system of linear equations over $\mathbb{F}_p$ which one checks to be equivalent to $c=0,a=d$. It follows that

$$\pi_0(\begin{pmatrix}a & b\\ c & d\end{pmatrix})=\pi_0(\begin{pmatrix}a & b\\ 0 & a\end{pmatrix})=\pi_0(\begin{pmatrix}1 & b/a\\ 0 & 1\end{pmatrix})\in\langle\alpha\rangle.$$

For (2): Note that by Lemma 4.3.1.3(2,ii), α is an element of $\mathrm{PGL}_2(q)$, and so by the element structure of $\mathrm{PGL}_2(q)$, α is conjugate in $\mathrm{PGL}_2(q)$ to an element of the form $\pi_0(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix})$ with $x \in \mathbb{F}_q^*$ of order $\frac{q-1}{2}$ (i.e., x generates the subgroup of squares in $\mathbb{F}_q^*$); it suffices to show that the centralizers in $\mathrm{Aut}(\mathrm{PSL}_2(q))$ of such elements are contained in $\mathrm{PGL}_2(q)$. We do so by contradiction: Assume that for some nontrivial field automorphism $\sigma = \mathrm{Frob}^e$ of $\mathbb{F}_q$, where Frob denotes the Frobenius automorphism of $\mathbb{F}_q$ and $1 \leq e < f$, and for some $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{GL}_2(q)$, we have

$$\pi_0(A\sigma \cdot \begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix} \cdot \sigma^{-1}A^{-1}) = \pi_0(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix}). \tag{4}$$

Easy computations reveal that (4) is equivalent to the existence of some $\lambda \in \mathbb{F}_q^*$ such that

$$\frac{1}{ad-bc} \cdot \begin{pmatrix}ad-\sigma(x)bc & ab(\sigma(x)-1)\\ cd(1-\sigma(x)) & \sigma(x)ad-bc\end{pmatrix} = \lambda \cdot \begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix}. \tag{5}$$

Comparing the coefficients in the bottom left and top right corners in (5), we find that $ab = 0$ and $cd = 0$, so either $a = d = 0$ or $b = c = 0$. In the latter case, comparing the coefficients in the top left corners of (5) yields $\lambda = 1$, and thus comparing the bottom right coefficients in (5), we get that $\sigma(x) = x$, which implies $\frac{p^f-1}{2} \mid p^e - 1$, or $p^f - 1 \mid 2(p^e - 1)$, although $p^f - 1 > p^f - p = p \cdot (p^{f-1} - 1) > 2 \cdot (p^e - 1)$, a contradiction. In the first case, comparing the coefficients in the top left corners of (5) gives $\lambda = \sigma(x)$, and thus by comparing the coefficients in the bottom right corners of (5), $\sigma(x) = x^{-1}$, which implies $\frac{p^f-1}{2} \mid p^e + 1$, or $p^f - 1 \mid 2(p^e + 1)$, although it is easy to check that $2(p^e + 1) \leq 2(p^{f-1} + 1) < p^f - 1$, a contradiction.
For (3): This can be treated with an argument analogous to the one for (2) (of course, except for the cases $q = 9, 25$, the statement immediately follows from (2)).
For (4): Consider the natural embedding

$$\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \hookrightarrow \mathrm{PGL}_2(q^2) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p) = \mathrm{Aut}(\mathrm{PSL}_2(q^2))$$

extending the natural embedding $\mathrm{PGL}_2(q) \hookrightarrow \mathrm{PGL}_2(q^2)$, by means of which we view $\mathrm{Aut}(\mathrm{PSL}_2(q))$ as a subgroup of $\mathrm{Aut}(\mathrm{PSL}_2(q^2))$. By Lemma 4.3.1.3(2,ii), $\alpha \in \mathrm{PGL}_2(q)$, and by the element structure of $\mathrm{PGL}_2(q)$, α is conjugate in $\mathrm{PGL}_2(q^2)$ to an element of the form $\pi_1(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix})$, where the order of $x \in \mathbb{F}_{q^2}^*$ is $\frac{q+1}{2}$. Denote by Frob the Frobenius automorphism of $\mathbb{F}_{q^2}$. It is sufficient to show that $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q^2))}(\pi_1(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix})) \subseteq \mathrm{PGL}_2(q^2) \rtimes \langle \mathrm{Frob}^f \rangle$, since this implies $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q^2))}(\alpha) \subseteq \mathrm{PGL}_2(q^2) \rtimes \langle \mathrm{Frob}^f \rangle$, and so

$$\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q))}(\alpha) = \mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(q^2))}(\alpha) \cap \mathrm{Aut}(\mathrm{PSL}_2(q)) \subseteq$$

$$\subseteq (\mathrm{PGL}_2(q^2) \rtimes \langle \mathrm{Frob}^f \rangle) \cap \mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q).$$

To see that among the elements of $\mathrm{Aut}(\mathrm{PSL}_2(q^2))$, $\pi_1(\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix})$ only commutes with elements from $\mathrm{PGL}_2(q^2) \rtimes \langle \mathrm{Frob}^f \rangle$, we proceed by contradiction, with the same ansatz as in point (2). This time, the divisibility relations at which one arrives in the two cases are $p^f + 1 \mid 2(p^e - 1)$ and $p^f + 1 \mid 2(p^e + 1)$ respectively. Note that now, $1 \leq e < 2f$, so we cannot argue as in point (2) that the supposed multiple is always smaller than the supposed divisor. However, this idea at least excludes the case $e < f$, so we may write $e = f + k$ with $0 \leq k < f$. Then it is easy to check that $2p^k - 1 < \frac{2(p^e-1)}{p^f+1} < 2p^k$, making the first inequality contradictory. Similarly, one can exclude the case $k > 0$ for the second inequality, leaving only the case $k = 0$, i.e., $e = f$.
For (5): This follows immediately from (4). □

Proof of Theorem 4.3.1.1. As pointed out before, point (1) of the theorem follows from Lemma 4.3.1.2(2), so we focus on the proof of point (2). Let $A = \mathrm{A}_{x,\alpha} \in \mathrm{Aff}(\mathrm{Aut}(\mathrm{PSL}_2(q)))$ be such that $\Lambda(A) = \Lambda_{\mathrm{aff}}(\mathrm{Aut}(\mathrm{PSL}_2(q)))$. Set $o_1 := \mathrm{ord}(\alpha)$ and $o_2 := \mathrm{ord}(\mathrm{sh}_\alpha(x))$, so that $\Lambda(A) = \mathrm{ord}(A) = o_1 \cdot o_2$, and note that $o_1, o_2 \leq q+1$.

If q is prime, then on the one hand, we cannot have $o_1 = o_2 = q+1$, since that would imply by Lemma 2.1.6 that $(q+1)^2 \mid |\mathrm{Aut}(\mathrm{PSL}_2(q))| = |\mathrm{PGL}_2(q)| = q(q^2-1)$, a contradiction. The next smaller potential order of A is $q(q+1)$, which is indeed attained by Lemma 2.1.8 and the fact that $\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q)$ contains both an element of order q and of order $q+1$.

If $q = 2^f$ with $f \geq 3$, then Lemma 2.1.6 again excludes the case $o_1 = o_2 = q+1 = 2^f+1$. By Lemma 4.3.1.3(1), the next smaller potential order of A is $(q+1)\cdot(q-1) = q^2-1$, which can be attained in view of Lemma 2.1.8.

Finally, consider the case $q = p^f$ with p an odd prime and $f \geq 2$. First, one verifies with GAP [3] that $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(\mathrm{PSL}_2(9))) = 40 = \frac{1}{2}(9^2-1)$ and $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(\mathrm{PSL}_2(25))) = 312 = \frac{1}{2}(25^2-1)$, so we may assume $(p,f) \notin \{(3,2),(5,2)\}$ from now on. By the element structure of $\mathrm{PGL}_2(q)$ and Lemma 2.1.8, it is clear that $\frac{1}{2}(q^2-1)$ can be attained as the order of some periodic affine map of $\mathrm{Aut}(\mathrm{PSL}_2(q))$, so it remains to show that $o_1 \cdot o_2 \leq \frac{1}{2}(q^2-1)$. We do this in a case distinction.

First assume that $o_1 = q+1$, so that by Lemma 4.3.1.3(2,ii), $\alpha \in \mathrm{PGL}_2(q)$. Then the inequality is equivalent to $o_2 \leq \frac{q-1}{2}$. If $o_2 > \frac{q-1}{2}$, by Lemma 4.3.1.3(2,ii) again, it follows that $o_2 \in \{q+1, q-1, \frac{q+1}{2}\}$. In each of these three cases, using Lemma 2.1.7 and Lemma 4.3.1.4(5,3,4) respectively, we conclude that $x \in \mathrm{PGL}_2(q)$. This gives a contradiction when $o_2 = q+1$ or $o_2 = q-1$, since by the fact that $[\mathrm{PGL}_2(q) : \mathrm{PSL}_(q)] = 2$ and o_1 is even, we get that $\mathrm{sh}_\alpha(x) \in \mathrm{PSL}_2(q)$, but $\mathrm{PSL}_2(q)$ does not have any elements of order $q+1$ or $q-1$. The case $o_2 = \frac{q+1}{2}$ can be refuted by Lemma 2.1.6 (applied to $G := \mathrm{PGL}_2(q)$) again.

Next assume that $o_1 = q-1$, in which case $\alpha \in \mathrm{PGL}_2(q)$ as well. The inequality is equivalent to $o_2 \leq \frac{q+1}{2}$, so it remains to exclude the two cases $o_2 = q+1$ and $o_2 = q-1$, which can be done as in the previous case, deriving the contradictory $\mathrm{sh}_\alpha(x) \in \mathrm{PSL}_2(q)$.

If $o_1 = \frac{q+1}{2}$, we only need to exclude the case $o_2 = q+1$, which can be done as in the case $o_1 = q+1$ using Lemma 2.1.6. Finally, if $o_1 \leq \frac{q-1}{2}$, then the inequality holds for sure. □

Theorem 4.3.1.1 implies by some easy computations that for primary $q \geq 5$, $\Lambda_{\mathrm{aff}}(\mathrm{PSL}_2(q)) > |\mathrm{PSL}_2(q)|^{\frac{2}{3}}$ if and only if q is a prime, in which case $\Lambda_{\mathrm{aff}}(\mathrm{PSL}_2(q)) = q(q+1)$, and verification of the statement about monotonous convergence of the upper bound is also easy. This settles our discussion of the subcase $n = 1$.

4.3.2 Useful observations for the other subcases

The following lemma is immediate from the element structure of $\mathrm{PGL}_2(p)$:

Lemma 4.3.2.1. *Let $p \geq 5$ be a prime, and let $A \in \mathrm{Aff}(\mathrm{Aut}(\mathrm{PSL}_2(p))) = \mathrm{Aff}(\mathrm{PGL}_2(p))$. Then $\mathrm{ord}(A)$ is a divisor of one of the following: $p(p+1), p(p-1), p^2-1$.* □

Another useful observation (similar in spirit to Lemma 2.4.2(2)) is the following: Since we have $\Lambda(\mathrm{Aut}(\mathrm{PSL}_2(q)^n)) = \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^n))$, and $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(\mathrm{PSL}_2(q)^n)) \leq \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^n))^2$, whenever $\Lambda(\mathrm{Aut}(\mathrm{PSL}_2(q)^n)) \leq |\mathrm{PSL}_2(q)|^{\frac{n}{3}}$, we also have $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(\mathrm{PSL}_2(q)^n)) \leq |\mathrm{PSL}_2(q)|^{\frac{2n}{3}}$.

4.3.3 Subcase: $n = 2$

Clearly, for primes $p \geq 5$, $\Lambda(\mathrm{Aut}(\mathrm{PSL}_2(p)^2)) = \Lambda(\mathrm{Aut}(\mathrm{PSL}_2(p)) \wr \mathcal{S}_2)$ is bounded from below by $p(p+1) = \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(p))^2)$, and by Lemma 2.3.2, elements from $\mathrm{Aut}(\mathrm{PSL}_2(p)^2) \backslash \mathrm{Aut}(\mathrm{PSL}_2(p))^2$ have order bounded from above by $2\cdot(p+1) < p(p+1)$, so indeed, we have $\Lambda(\mathrm{Aut}(\mathrm{PSL}_2(p)^2)) = \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(p)^2)) = p(p+1)$. As for $q \geq 5$ that are not prime, we first verify directly with GAP [3] that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(9)^2)) = 40 < 360^{2/3}$. For all other odd q, we can use Lemma 4.3.1.3(2,ii) to see that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^2)) = \frac{1}{2}(q^2-1) < (\frac{1}{2}q(q^2-1))^{\frac{2}{3}}$, and Lemma 2.3.2 to treat automorphisms outside $\mathrm{Aut}(\mathrm{PSL}_2(q)^2)$ as before. Finally, for $q = 2^f$ with $f \geq 3$, by Lemma 4.3.1.3(1), we have $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^2)) = q^2-1 < (q(q^2-1))^{\frac{2}{3}}$, and we can treat all other automorphisms by Lemma 2.3.2 again.

As for Λ_{aff}-values in the subcase $n = 2$, by the "useful observation" after Lemma 4.3.2.1, it remains to show that $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(\mathrm{PSL}_2(p)^2)) \leq |\,\mathrm{PSL}_2(p)|^{\frac{4}{3}}$ for primes $p \geq 5$. It is easily checked with GAP [3] that $\Lambda_{\mathrm{aff}}(\mathrm{Aut}(\mathrm{PSL}_2(5)^2)) = 120 < 60^{\frac{4}{3}}$, so we may assume $p \geq 7$ from now on. Let $A = \mathrm{A}_{x,\alpha} \in \mathrm{Aff}(\mathrm{Aut}(\mathrm{PSL}_2(p)^2))$. We know that we can identify α with an element in $\mathrm{Aut}(\mathrm{PSL}_2(p)^2)$, that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(p))^2) = p(p+1)$ and that elements from $\mathrm{Aut}(\mathrm{PSL}_2(p)^2) \backslash \mathrm{Aut}(\mathrm{PSL}_2(p))^2$ have at most the order $2 \cdot (p+1)$. Therefore, if not both $\alpha, \mathrm{sh}_\alpha(x) \in \mathrm{Aut}(\mathrm{PSL}_2(p))^2$, then the order of A is at most $2(p+1) \cdot p(p+1) < (\frac{1}{2}p(p^2-1))^{\frac{4}{3}}$. So we may assume $\alpha, \mathrm{sh}_\alpha(x) \in \mathrm{Aut}(\mathrm{PSL}_2(p))^2$ from now on, and also $\mathrm{ord}(A) > 2(p+1) \cdot p(p+1)$. The latter implies that the two components of $\mathrm{sh}_\alpha(x)$ must be of different order. But conjugation of $\mathrm{sh}_\alpha(x)$ by any element from $\mathrm{Aut}(\mathrm{PSL}_2(p)^2) \setminus \mathrm{Aut}(\mathrm{PSL}_2(p)^2)$ swaps the orders of the components, and so $\mathrm{sh}_\alpha(x)$ cannot commute with any such element. In other words, $\mathrm{C}_{\mathrm{Aut}(\mathrm{PSL}_2(p)^2)}(\mathrm{sh}_\alpha(x)) \subseteq \mathrm{Aut}(\mathrm{PSL}_2(p))^2$, and so, by an application of Lemma 2.1.7, we conclude that $x \in \mathrm{Aut}(\mathrm{PSL}_2(p))^2$. Together with $\alpha \in \mathrm{Aut}(\mathrm{PSL}_2(p))^2$, this implies that A decomposes as a product $A_1 \times A_2$, with $A_1, A_2 \in \mathrm{Aff}(\mathrm{Aut}(\mathrm{PSL}_2(p)))$. Therefore, by Lemma 4.3.2.1, $\mathrm{ord}(A) = \mathrm{lcm}(\mathrm{ord}(A_1), \mathrm{ord}(A_2)) \leq p(p^2-1) < (\frac{1}{2}p(p^2-1))^{\frac{4}{3}}$.

4.3.4 Subcase: $n = 3$

Denote by $\pi_3 : \mathrm{Aut}(\mathrm{PSL}_2(q)^3) = \mathrm{Aut}(\mathrm{PSL}_2(q)) \wr \mathcal{S}_3 \to \mathcal{S}_3$ the canonical projection. By a simple case distinction according to the cycle type of $\pi_3(\alpha)$, Lemma 2.3.2 can be used to show that automorphisms α outside $\mathrm{Aut}(\mathrm{PSL}_2(q))^3$ have order bounded from above by $2q(q+1) < |\,\mathrm{PSL}_2(q)|$ in all cases. If q is a prime, then since the element orders in $\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q)$ are just the divisors of $q+1, q$ and $q-1$, we have $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q))^3) = \mathrm{lcm}(q+1, q, q-1) = \frac{1}{2}q(q^2-1) = |\,\mathrm{PSL}_2(q)|^{\frac{3}{3}}$. If $q = 2^f$ with $f \geq 3$, by Lemma 4.3.1.3(1), we have $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^3)) < (q+1)(q-1)^2 < |\,\mathrm{PSL}_2(q)|$. For $q = 9$, one checks with GAP [3] that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(9)^3)) = 120 < 360$, and for odd $q \geq 25$, using Lemma 4.3.1.3(2,ii), we conclude that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q))^3) < \frac{1}{2}(q+1)(q-1)^2 < |\,\mathrm{PSL}_2(q)|$.

4.3.5 Subcase: $n = 4$

We will show $\Lambda(\mathrm{Aut}(\mathrm{PSL}_2(q)^4)) < |\,\mathrm{PSL}_2(q)|^{\frac{4}{3}}$ for all primary $q \geq 5$. For $q = 5$, one can check directly that $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(5))^4) = 60 < 60^{\frac{4}{3}}$, and automorphisms α from outside $\mathrm{Aut}(\mathrm{PSL}_2(5))^4$ are treated with Lemma 2.3.2 like before. Assuming $q \geq 7$, we have $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_2(q)^4)) \leq g(4) \cdot \exp(\mathrm{Aut}(\mathrm{PSL}_2(q))) \leq 4 \cdot \log_p(q) \cdot p \cdot \frac{q^2-1}{\gcd(2,q-1)} \leq 4 \cdot |\,\mathrm{PSL}_2(q)| < |\,\mathrm{PSL}_2(q)|^{\frac{4}{3}}$.

4.3.6 Subcase: $n \geq 5$

Here we can use crude upper bounds and "get away with it"; it is sufficient and easy to verify that

$$\Lambda(\mathrm{Aut}(\mathrm{PSL}_2(q)^n)) \leq g(n) \cdot \exp(\mathrm{Aut}(\mathrm{PSL}_2(q))) < 3^{\frac{n}{3}} \cdot |\,\mathrm{PSL}_2(q)| \leq |\,\mathrm{PSL}_2(q)|^{n/3}.$$

4.4 Case: $S = \mathrm{PSL}_d(q), d \geq 3, q \geq 2$

From now on, we will always work with Lemma 2.4.2(2). Furthermore, we will use the information on maximum automorphism orders of finite simple groups from [5, Table 3]. Note that since $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$, we may assume that $(d,q) \neq (3,2)$, and so $\mathrm{mao}(\mathrm{PSL}_d(q)) = \frac{q^d-1}{q-1}$. In view of $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_d(q))^n) \leq \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_d(q)))^n$, our goal is to show that

$$g(n) \cdot \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_d(q)))^n < |\,\mathrm{PSL}_d(q)|^{\frac{n}{3}} = (\frac{q^{d(d-1)/2}}{\gcd(d,q-1)} \cdot \prod_{i=2}^{d}(q^i-1))^{\frac{n}{3}}. \tag{6}$$

4.4.1 Subcase: $d = 3$

We need to treat the subsubcases $q = 3$ and $q = 4$ separately. Using GAP [3], one finds that the list of element orders in $\mathrm{Aut}(\mathrm{PSL}_3(3))$ is $1, 2, 3, 4, 6, 8, 12, 13$. This implies that

$$g(1) \cdot \mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_3(3))^1) = 1 \cdot 13 < 5616^{\frac{1}{3}},$$

that

$$g(2)\cdot\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_3(3)^2)=2\cdot 156<5616^{\frac{2}{3}},$$

and that $g(n)\cdot\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_3(3)^n))=g(n)\cdot 312<5616^{n/3}$ for $n\geq 3$. The subsubcase $q=4$ is treated analogously.

For $q\geq 5$, using Proposition 2.4.1, we see that for proving (6), it is sufficient to show

$$(q^2+q+1)^2<\frac{q^3}{3\gcd(3,q-1)}\cdot(q-1)(q^2-1),$$

which is easy to verify.

4.4.2 Subcase: $d=4$ or $d=5$

For $d=4$, splitting the factor $(q^2)^{\frac{n}{3}}$ from the beginning of the right-hand side of (6), we can "swallow" the factor $g(n)$ on the left-hand side by Proposition 2.4.1, and see that it is sufficient to show that

$$(q^3+q^2+q+1)^2<\frac{q^4}{\gcd(4,q-1)}(q-1)(q^3-1)(q^2-1). \tag{7}$$

Replacing the left-hand side of (7) by the larger q^8, dividing both sides by q^8 and performing appropriate cancelations and distributions of factors q among the factors on the right-hand side, we get the stronger inequality

$$1<\frac{1}{\gcd(4,q-1)}(q-1)\cdot(\sqrt{q}-\frac{1}{q^{5/2}})\cdot(\sqrt{q}-\frac{1}{q^{3/2}}), \tag{8}$$

which is obviously true. The subcase $d=5$ can be treated in a similar way.

4.4.3 Subcase: $d\geq 6$

One can check that $2d\leq\frac{d(d-1)}{2}-2$ for $d\geq 6$. The left-hand side of (6) is therefore bounded from above by

$$(q^2)^{\frac{n}{3}}\cdot(q^d-1)^n<(q^2)^{\frac{n}{3}}\cdot(q^d-1)^{\frac{n}{3}}\cdot(q^{2d})^{\frac{n}{3}}\leq(q^2)^{\frac{n}{3}}\cdot(q^d-1)^{\frac{n}{3}}\cdot(q^{\frac{d(d-1)}{2}-2})^{\frac{n}{3}}=(q^{d(d-1)/2}\cdot(q^d-1))^{\frac{n}{3}},$$

which is obviously smaller than the right-hand side of (6).

4.5 Case: $S=\mathrm{PSU}_d(q), d\geq 3, (d,q)\neq(3,2)$

Note that $|\mathrm{PSU}_d(q)|=\frac{1}{\gcd(d,q+1)}q^{d(d-1)/2}\prod_{i=2}^{d}(q^i-(-1)^i)$.

4.5.1 Subcase: $d=3$

It follows from [5, Table 3] that $\mathrm{mao}(\mathrm{PSU}_3(q))\leq q^2+q$, and so it is sufficient to show that

$$g(n)\cdot(q^2+q)^n<(\frac{1}{\gcd(3,q+1)}q^3(q^3+1)(q^2-1))^{\frac{n}{3}}. \tag{9}$$

Splitting $q^{\frac{n}{3}}$ from the right-hand side of (9) to "swallow" $g(n)$, we see that (9) is implied by

$$\gcd(3,q+1)<\frac{q^2-q+1}{q+1}\cdot(1-\frac{1}{q}). \tag{10}$$

For $q\geq 7$, the first factor on the right-hand side of (10) is bounded from below by 4, and so the entire right-hand side is bounded from below by $4\cdot\frac{6}{7}>3\geq\gcd(3,q+1)$. For $q=3$ and $q=4$, one verifies the validity of (10) directly. Finally, for $q=5$, one can check that

$$g(n)\cdot\mathrm{meo}(\mathrm{Aut}(\mathrm{PSU}_3(5))^n)<126000^{\frac{n}{3}},$$

like we did for $q=3$ in the subcase $d=3$ of the previous case (Subsubsection 4.4.1).

4.5.2 Subcase: $d \geq 4$

We read off from [5, Table 3] that $\operatorname{mao}(\mathrm{PSU}_4(q)) \leq q^3+4$, so for the subsubcase $d=4$, we want to show that

$$g(n) \cdot (q^3+4)^n < (\frac{q^6}{\gcd(4,q+1)}(q^4-1)(q^3+1)(q^2-1))^{\frac{n}{3}}. \tag{11}$$

Splitting $(q+1)^{\frac{n}{3}}$ from the right-hand side of (11) to "swallow" $g(n)$, we see that (11) is weaker than

$$(q^3+4)^3 < \frac{q^6}{\gcd(4,q+1)}(q^4-1)(q^3+1)(q-1),$$

which is easy to prove for all $q \geq 2$. The subsubcase $d=5$ is similar to $d=4$, using that $\operatorname{mao}(\mathrm{PSU}_5(q)) < q^5$. Finally, using $\operatorname{mao}(\mathrm{PSU}_d(q)) < q^d$, we can treat the subsubcase $d \geq 6$ similarly to the subcase $d \geq 6$ of the previous case (Subsubsection 4.4.3).

4.6 Case: $S = \mathrm{PSp}_{2m}(q), m \geq 2, (m,q) \neq (2,2)$ or $S = \mathrm{P}\,\Omega_{2m+1}(q), m \geq 3$

By [5, Table 3], in both cases, $\operatorname{mao}(S) \leq \frac{q^{m+1}}{q-1}$. Also, $|S| = \frac{q^{m^2}}{\gcd(2,q-1)}\prod_{i=1}^{m}(q^{2i}-1)$ in both cases, so we can discuss them simultaneously. We want to show that

$$g(n) \cdot \frac{q^{n(m+1)}}{(q-1)^n} < (\frac{q^{m^2}}{\gcd(2,q-1)}\prod_{i=1}^{m}(q^{2i}-1))^{\frac{n}{3}}. \tag{12}$$

Split a factor $(q+1)^{\frac{n}{3}}$ from the right-hand side of (12) to "swallow" $g(n)$. It follows that (12) is weaker than

$$q^{3(m+1)} < \frac{q^{m^2}}{\gcd(2,q-1)}\prod_{i=2}^{m}(q^{2i}-1) \cdot (q-1)^4, \tag{13}$$

which is easy to verify for all $(m,q) \neq (2,2)$.

4.7 Case: $S = \mathrm{P}\,\Omega_{2m}^{+}(q), m \geq 4$ or $S = \mathrm{P}\,\Omega_{2m}^{-}(q), m \geq 4$

In both cases, we have $\operatorname{mao}(S) \leq \frac{q^{m+1}}{q-1}$ and $|S| = \frac{q^{m(m-1)}(q^m-1)}{\gcd(4,q^m-1)}\prod_{i=1}^{m-1}(q^{2i}-1)$, so we want to show that

$$g(n) \cdot \frac{q^{n(m+1)}}{(q-1)^n} < (\frac{q^{m(m-1)}(q^m-1)}{\gcd(4,q^m-1)}\prod_{i=1}^{m-1}(q^{2i}-1))^{\frac{n}{3}}, \tag{14}$$

which can be done analogously to the previous case (Subsection 4.6).

4.8 Case: S is an exceptional group of Lie type

Guest, Morris, Praeger and Spiga [5, Proof of Theorem 1.2] derived upper bounds on $\operatorname{mao}(S)$ for such S, based on the information on largest element orders of exceptional Lie type groups of odd characteristic from [7, Table A.7], the upper bounds on largest element orders for those of even characteristic from [5, Table 5], and information on outer automorphism group orders of such groups from [2, Table 5, p. xvi]. Denoting their upper bound by $o(S)$, one can, in almost all cases, prove the sufficient inequality

$$g(n) \cdot o(S)^n < |S|^{\frac{n}{3}} \tag{15}$$

with arguments similar to those used in the nonexceptional cases. There are two particular subcases where we use a sharper upper bound on $\operatorname{mao}(S)$, based on reading off the precise value of $\operatorname{meo}(S)$ (not just an upper bound on it) and of $|\operatorname{Out}(S)|$ from [2] and setting $o(S) := \operatorname{meo}(S) \cdot |\operatorname{Out}(S)|$. These two cases are $S = {}^3D_4(2)$ (with $o(S) = 18 \cdot 3 = 54$) and $S = {}^2F_4(2)'$ (with $o(S) = 16 \cdot 2 = 32$).

5 Acknowledgements

The author would like to thank the following people: Michael Giudici for raising his awareness to the paper [4], Igor Shparlinski and Alina Ostafe for a valuable discussion stimulating this improved version of a previous paper by the author, and Peter Hellekalek for his support and helpful comments.

References

[1] A. Bors, Classification of finite group automorphisms with a large cycle, preprint, arXiv:1410.2284.

[2] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985 (reprinted 2013).

[3] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.5*, 2014, `http://www.gap-system.org`.

[4] M. Giudici, C.E. Praeger and P. Spiga, Finite primitive permutation groups and regular cycles of their elements, *J. Algebra* **421**:27–55, 2015.

[5] S. Guest, J. Morris, C.E. Praeger and P. Spiga, On the maximum orders of elements of finite almost simple groups and primitive permutation groups, *Trans. Amer. Math. Soc.*, to appear, arXiv:1301.5166 [math.GR].

[6] M.V. Horoševskiĭ, On automorphisms of finite groups, *Math. USSR Sb.* **22**(4):584–594, 1974.

[7] W.M. Kantor and Á. Seress, Large element orders and the characteristic of Lie-type simple groups, *J. Algebra*, **322**(3):802–832, 2009.

[8] J.-P. Massias, Majoration explicite de l'ordre maximum d'un élément du groupe symétrique, *Ann. Fac. Sci. Toulouse Math. (5)* **6**(3–4):269–281, 1985.

[9] D.J.S. Robinson, *A Course in the Theory of Groups*, Springer (Graduate Texts in Mathematics, 80), New York, 2nd ed. 1996.

[10] J.S. Rose, Automorphism groups of groups with trivial centre, *Proc. London Math. Soc. (3)* **31**(2):167–193, 1975.

[11] J.B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6**:64–94, 1962.